

普通高等教育“十一五”国家级规划教材 计算机系列教材

网络技术与安全管理

申怀亮 申一鸣 编著

清华大学出版社

计算机系列教材

网络技术与安全管理

申怀亮　申一鸣　编著

清华大学出版社
北　京

内 容 简 介

本书对网络技术与安全管理做了全面介绍。全书共 10 章,内容包括计算机网络发展历程、组成及分类,开放系统互连参考模型 OSI/RM、Internet 网络 TCP/IP 体系结构,计算机局域网技术,网络数据通信基础,通信介质以及网络设备与功能,网络操作系统,Windows Server 2008 网络服务器基本配置,计算机网络安全管理以及网络安全管理工具软件应用等。

本书从实际应用出发,在理论基础上,每章有针对性地安排了实际操作内容,如 Visio 绘制网络拓扑图、局域网打印机共享、双绞线制作、对等网络组建、交换机路由器基本配置等,特别是基于 Windows Server 2008 网络操作系统的网络服务器配置与管理,有助于强化读者对网络应用技能的全面提高。

本书可作为高职高专院校计算机及网络相关专业的教材,也可作为计算机网络管理技术人员的参考书以及社会培训的教材。

图书在版编目(CIP)

网络技术与安全管理/申怀亮,申一鸣编著. —北京:清华大学出版社,2014
计算机系列教材
ISBN 978-7-302-36182-4

Ⅰ. ①网… Ⅱ. ①申… ②申… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2014)第 072618 号

责任编辑: 白立军 战晓雷
封面设计:
责任校对: 白 蕾
责任印制:

出版发行: 清华大学出版社
网 址: http://www.tup.com.cn, http://www.wqbook.com
地 址: 北京清华大学学研大厦 A 座 **邮 编:** 100084
社 总 机: 010-62770175 **邮 购:** 010-62786544
投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载: http://www.tup.com.cn,010-62795954
印 刷 者:
装 订 者:
经 销: 全国新华书店
开 本: 185mm×260mm **印 张:** 14.5 **字 数:** 335 千字
版 次: 2014 年 月第 1 版 **印 次:** 2014 年 月第 1 次印刷
印 数: 1~ 000
定 价: .00 元

产品编号:058870-01

前 言

从 20 世纪 70 年代起，以互联网为代表的计算机网络得到迅猛发展，在几十年的发展历程中，计算机网络作为现代通信技术与计算机技术高度融合的产物，经历了从简单到复杂、从低级到高级、从地区到全球的发展过程，对此本书给出了较为详细的描述。本书内容主要包括计算机网络基础知识、计算机网络体系结构与网络协议、计算机局域网技术、网络数据通信基础、通信介质及主要特征、网络通信设备及功能、网络操作系统、Windows Server 2008 网络服务器配置与管理、计算机网络安全与管理及网络安全管理工具软件等内容。

本书在编著过程中努力实现下列几点：

(1) 力求理论知识系统完整。本书的目标是作为高职高专学生学习计算机网络技术的基础教材，也可作为计算机网络管理技术人员的参考书，理论基本知识系统完整，有利于为学习者奠定较好的基础。

(2) 努力实现在解决实际问题中提升实践技能。计算机网络是应用技术的产物，学习网络技术的主要目的是充分应用网络技术，网络应用技术问题蕴藏在实际工作与生活中，本书给出的实践题均源自实际需要。

(3) 注重理论与实践的紧密结合。本书努力解决理论学习与实践应用相脱节的问题，对于计算机网络技术而言，理论是实践的先导，实践促进理论学习。作者在多年教学实践中体会到，有些教程过度强调实践操作，将要求掌握的理论知识碎化于实践训练项目中，实际并不利于初学者系统认识事物，只能是事倍功半。为此，本书在每章之后，根据本章讲解的理论知识与技术，安排了与之相关性比较强的实践训练内容。

感谢黄崇本教授的支持与鼓励，才使作者下决心将多年的教学讲稿整理付梓，贡献给读者。感谢作者的同事们在校本教材使用中提出的宝贵意见和建议。本教材在编写过程中参考了许多资料，在此向有关作者致以衷心感谢。

恳请读者对书中不妥之处批评指正。

作　者

2014 年 5 月

目 录

第 1 章　计算机网络概述

本章主要内容

- 计算机网络的发展
- 计算机网络的组成
- 计算机网络的分类

20 世纪 70 年代,《第三次浪潮》(阿尔温·托夫勒著)一书描绘了信息社会的美好前景,从此为人类社会揭开了信息时代的序幕。目前,信息已经成为人们改造世界和推动世界发展的直接动力,以 Internet(因特网)为代表的信息网络作为现代社会最重要的信息基础设施之一,已经渗透到社会的各个领域,成为国家进步和社会发展的重要支柱,是知识经济的基础载体和支撑环境。

计算机网络是计算机技术与通信技术紧密结合的产物。随着经济全球化和社会信息化日益发展,在全球信息化浪潮的冲击下,人类对通信容量、通信业务的种类和通信质量的要求不断增长,计算机网络将为人类社会进入一个前所未有的信息时代提供保障。

1.1　计算机网络的发展

计算机网络仅有几十年的发展历史,是现代通信技术与计算机技术快速发展、相互促进、高度融合的产物,计算机网络的发展经历了从简单到复杂、从低级到高级、从地区到全球的发展过程。按照通信技术和计算机技术结合方式的不同,计算机网络经历了终端式计算机网络、通信中心式计算机网络、体系结构标准化计算机网络和互联高速计算机网络 4 个典型的发展阶段。

1.1.1　终端式计算机网络

20 世纪 50 年代中期,计算机数量比较稀少,而且价格比较昂贵,少量的计算机被集中放置在计算中心。对于使用计算机的用户来说,要使用计算机就必须到计算中心,使用计算机的方式也较落后。为了方便用户的需要,在用户所在地安装终端,通过远程线路把计算机和终端连接起来,这就是第一代计算机网络,也称为面向终端式计算机网络,见图 1-1。当然,按照目前对计算机网络的评价标准,终端式计算机网络应当称为面向终端分布计算机系统。

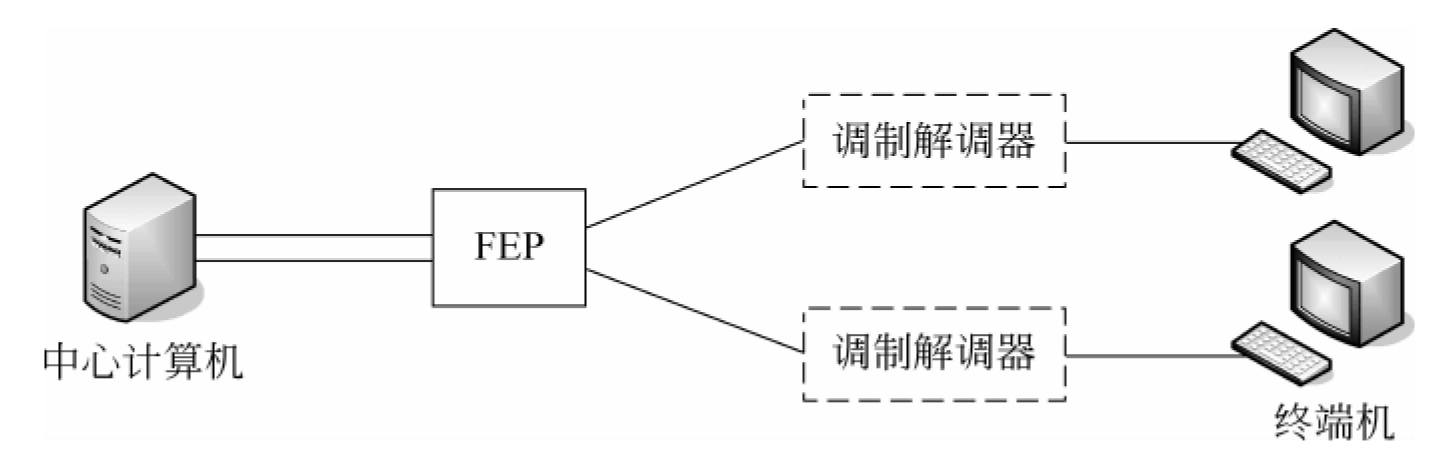


图 1-1　终端式计算机网络示意图

1.1.2　通信中心式计算机网络

20 世纪 60 年代，在面向终端网络蓬勃发展的同时，通信领域一场新的技术革命正在悄然进行，分组交换技术的出现为网络数据通信提供了技术支撑。美国国防部的高级研究计划局（ARPA）将分组交换技术应用于网络数据通信中，建立了世界上第一个采用分组交换技术的计算机网络 ARPANET，这就是因特网的前身。这种以通信网络为中心的计算机网络称为第二代计算机网络，见图 1-2，但这个时期的网络产品彼此之间是相互独立的，没有统一标准，各厂家提供的网络产品实现互连十分困难。

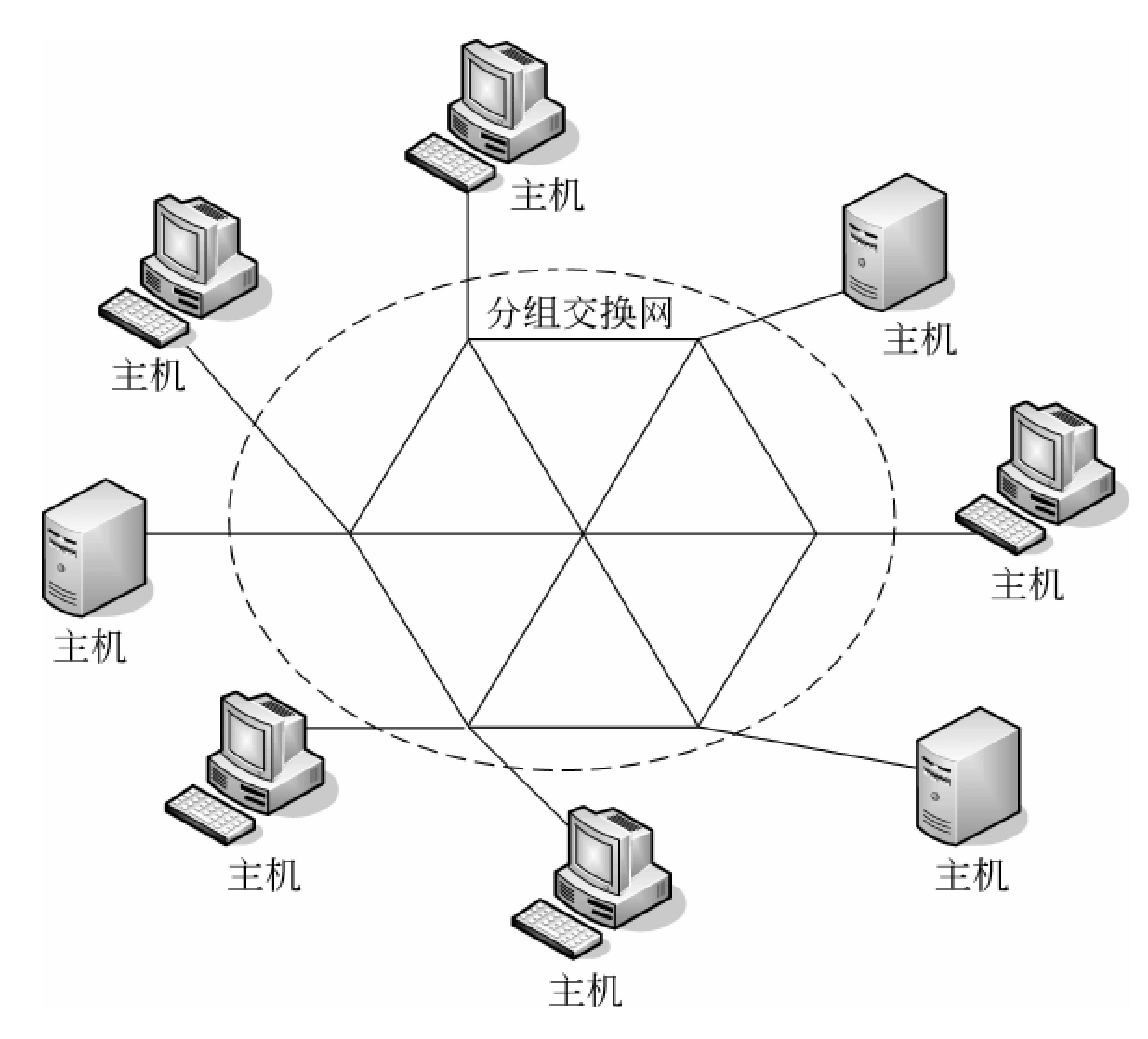


图 1-2　通信中心式计算机网络

1.1.3　体系结构标准化计算机网络

20 世纪 80 年代中期，计算机网络开始向体系结构标准化的方向迈进，即正式步入网络标准化时代。1989 年 2 月，国际标准化组织（ISO）正式颁布了一个开放系统互连参考

模型，即国际标准ISO 7498-2-1989。开放系统互连参考模型分为7个层次，也被称为ISO七层模型。从此网络产品有了统一的标准，为计算机网络技术迈向国际标准化方向奠定了基础，同时也为日后行业规范、有序地竞争提供了保障。

随着微机的广泛使用，局域网(LAN)获得了迅速发展。美国电气与电子工程师协会(IEEE)为了适应微机、个人计算机及局域网发展的需要，于1980年2月在旧金山成立了IEEE 802局域网络标准委员会，并制定了一系列局域网络标准。在此期间各种局域网大量涌现，特别是光纤局域网，光纤分布式数据接口(FDDI)网络标准及产品的相继问世，为推动计算机局域网络技术进步及应用奠定了良好的基础。这一阶段典型的标准化网络结构如图1-3所示，通信子网的交换设备主要是路由器和交换机。

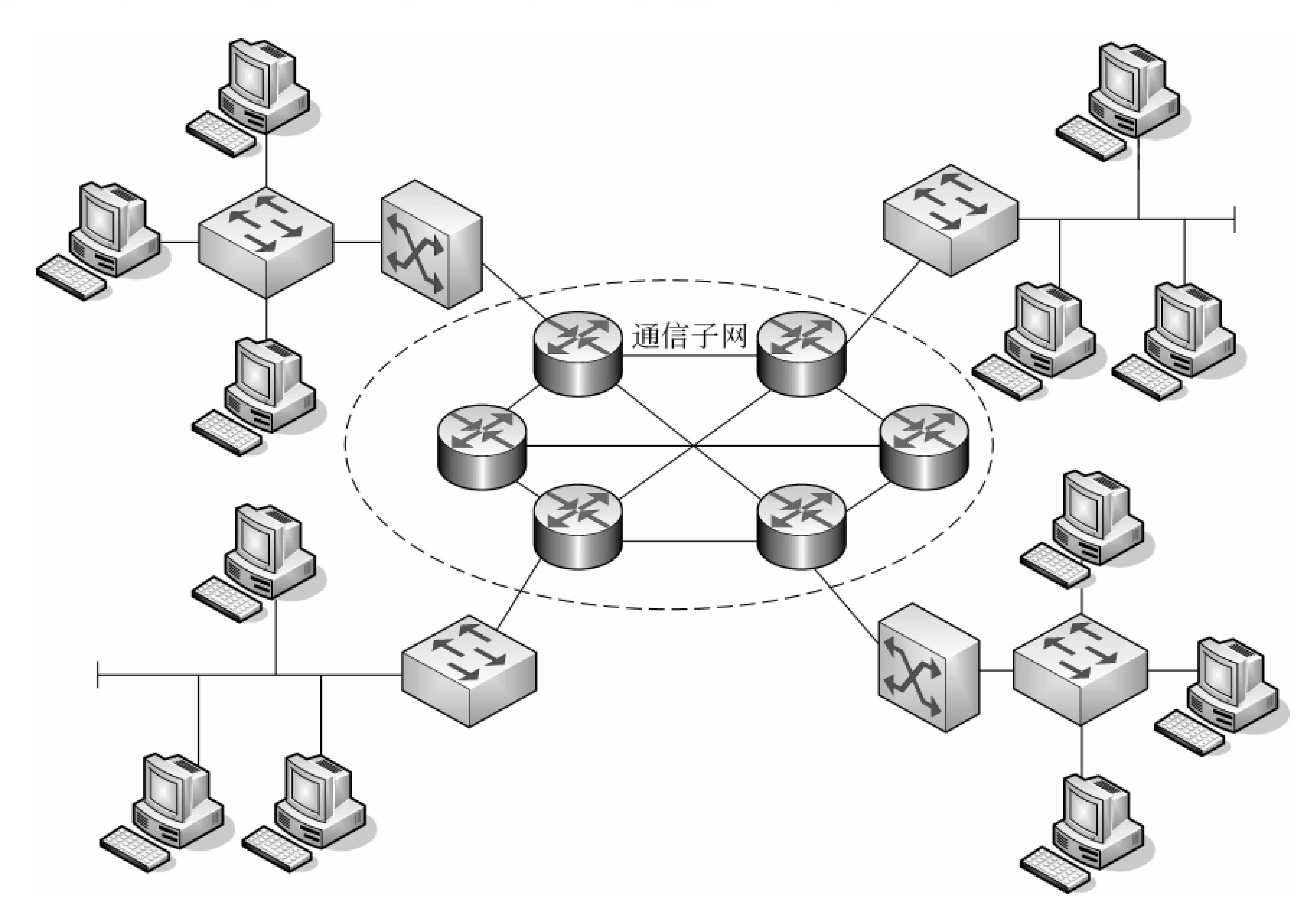


图1-3 体系结构标准化计算机网络

1.1.4 互联高速计算机网络

进入20世纪90年代，随着计算机网络技术的迅猛发展，特别是1993年美国宣布建立国家信息基础设施(NII)后，全世界许多国家纷纷制定本国的信息基础标准，从而极大地推动了计算机网络技术的发展，使计算机网络发展进入一个崭新的阶段，这就是计算机网络互联与高速网络阶段。

目前，全球以Internet为核心的高速计算机互联网络已经形成，Internet已经成为人类最重要的、最大的知识宝库。网络互联和高速计算机网络被称为第四代计算机网络，如图1-4所示。

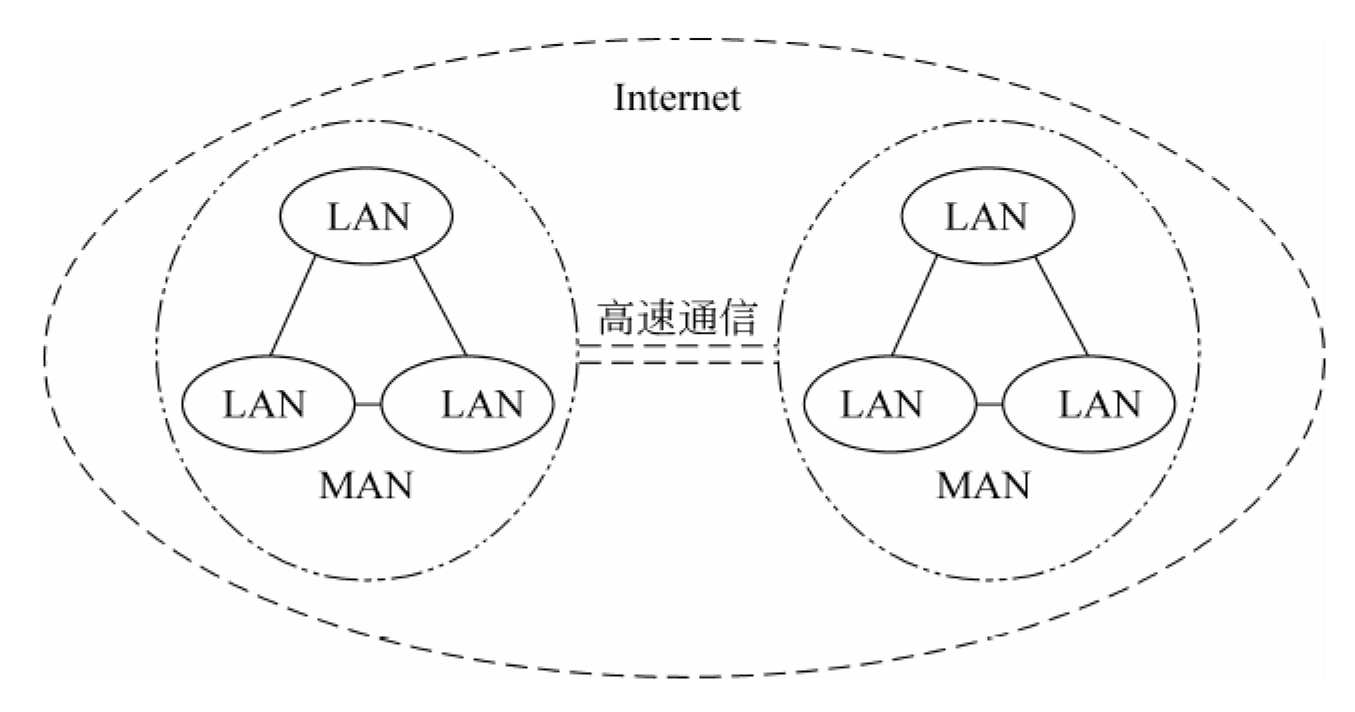


图 1-4　互联高速计算机网络示意图

1.2　计算机网络的组成

计算机网络是指把地理位置不同、系统功能独立的若干台计算机(主机,host)通过通信设备和线路连接起来,借助网络软件,实现网络数据通信和资源共享。因此,计算机网络一般按功能划分为两个主要组成部分:①负责数据处理业务,承担网络资源提供与服务的资源子网;②负责数据传输与交换控制,提供网络通信功能的通信子网。计算机网络的组成见图 1-5。

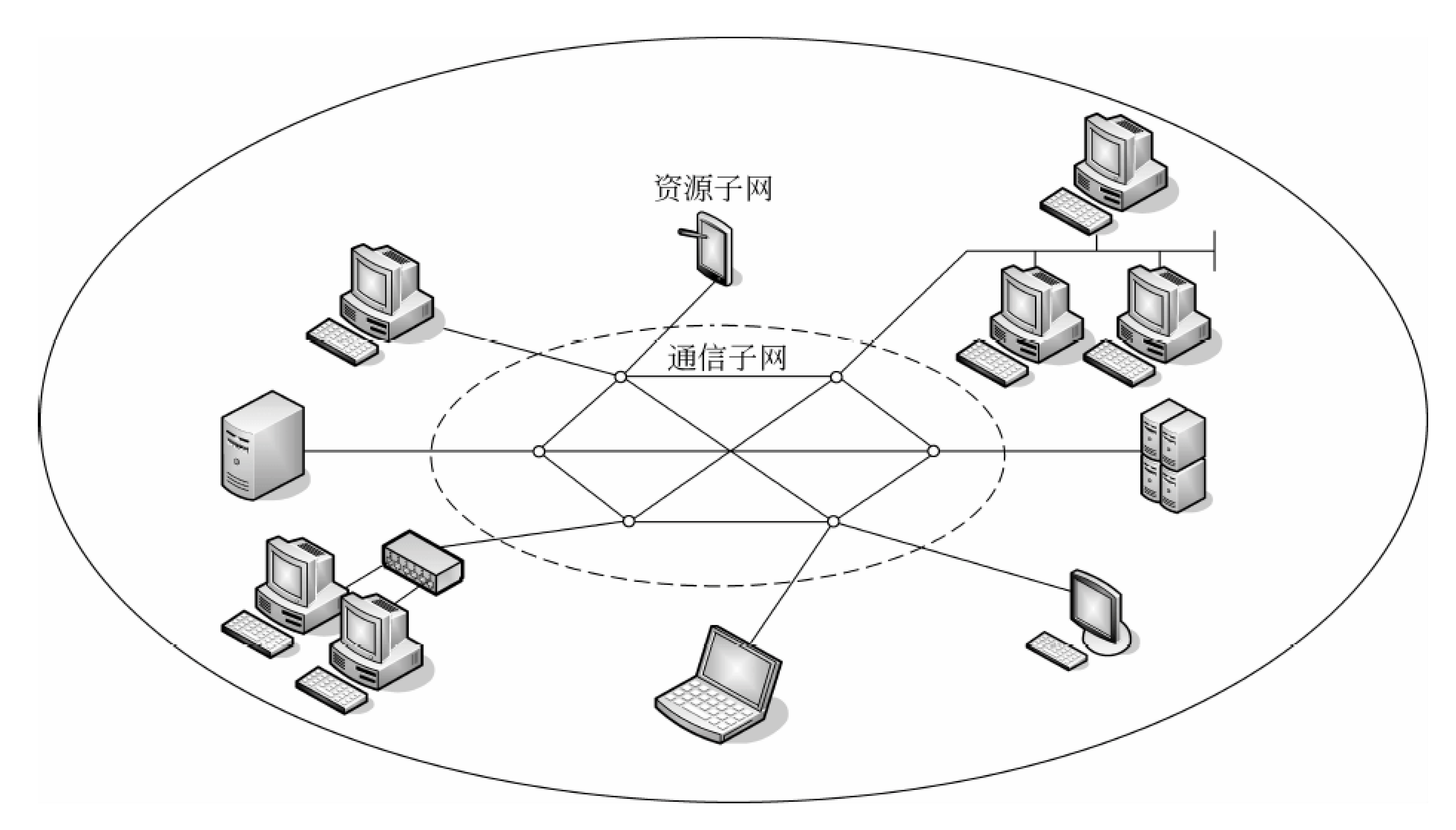


图 1-5　计算机网络的组成示意图

1.2.1　通信子网

通信子网提供网络通信功能,实现网络主机与主机之间的数据传输、交换控制与信号

转换等通信处理工作，通常由通信控制处理机（CCP）、通信线路与其他通信设备组成。

一般在网络拓扑结构中将通信控制处理机称为网络节点。它一方面作为与资源子网的主机和终端连接的接口，将主机和终端连入网内；另一方面又作为通信子网中的分组存储转发节点，完成分组的接收、校验、存储和转发等功能，实现将源主机信息准确发送到目的主机的作用。目前，通信控制处理机一般为路由器、交换机以及主机等。

通信线路为通信控制处理机与通信控制处理机之间、通信控制处理机与主机之间提供通信信道。计算机网络采用了多种通信线路，如电话线、双绞线、同轴电缆与光纤等有线通信信道，以及微波、远红外与卫星通信等无线通信信道。

1.2.2 资源子网

资源子网由主机系统、终端、终端控制器、联网外设、各种软件资源与信息资源组成。资源子网实现全网的面向应用的数据处理和网络资源共享，它由以下各种硬件和软件组成。

（1）主机系统。它是资源子网的主要组成单元，装有本地操作系统、网络操作系统、数据库和用户应用系统等软件。它通过高速通信线路与通信子网的通信控制处理机相连接。普通用户终端通过主机系统连入网内。

（2）终端。它是用户访问网络的界面。终端可以是简单的输入输出终端，也可以是带有微处理器的智能终端。智能终端除具有输入输出信息的功能外，本身具有存储与处理信息的能力。终端可以通过主机系统连入网内，也可以通过终端设备控制器或通信控制处理机连入网内。

（3）网络操作系统。它是建立在各主机操作系统之上的一个操作系统，用于实现不同主机之间的用户通信，以及全网硬件和软件资源的共享，并向用户提供统一的、方便的网络接口，便于用户使用网络。

（4）网络数据库。它是建立在网络操作系统之上的一种数据库系统，可以集中驻留在一台主机上，称作集中式网络数据库系统；也可以分布在每台主机上，称作分布式网络数据库系统，它向网络用户提供存取和修改网络数据库的服务，以实现网络数据库的共享。

（5）应用系统。它是应用上述系统软硬件、面向用户开发的应用系统，以满足用户的需求，是网络中最直接的资源。

1.2.3 现代网络结构的特点

在现代的广域网结构中，随着使用主机系统用户的减少，资源子网的概念已经有了变化。目前，通信子网由交换设备与通信线路组成，它负责完成网络中数据的传输与转发任务。通信子网的交换设备主要是路由器与交换机。随着微型计算机的广泛应用，连入局域网的微型计算机数目日益增多，它们一般通过路由器将局域网与广域网相连接。

另外，从网络层次角度看，网络的组成结构不再是一种简单的平面结构，而是发展成一种典型的3层网络结构，即核心层、汇聚层和接入层。

(1) 核心层。是网络的高速交换主干，是网络的枢纽中心，对整个网络的连通起到至关重要的作用。

(2) 汇聚层。是网络接入层和核心层的中间层，其作用是在主机接入核心层之前先做汇聚，以减轻核心层设备的负荷。汇聚层具有实施策略、安全、工作组接入、虚拟局域网(VLAN)之间的路由、源地址或目的地址过滤等多种功能。在汇聚层中，应该采用支持三层交换技术和VLAN的交换机，以达到网络隔离和分段的目的。

(3) 接入层。向本地网段提供主机接入。在接入层中，可以减少同一网段的主机数量，能够向工作组提供高速带宽。接入层可以选择不支持VLAN和三层交换技术的普通交换机。

1.3 计算机网络的分类

计算机网络可以从不同的角度进行分类，一般可按网络覆盖的地理范围分类、按网络的拓扑结构分类、按传输技术分类以及按网络的应用领域分类等。

1.3.1 按覆盖地理范围分类

计算机网络按其覆盖的地理范围分类是最常用的分类方法，也是比较容易理解的分类方法。按照网络覆盖的地理范围的大小，可以把计算机网络划分为局域网(LAN)、城域网(MAN)和广域网(WAN)3种类型。

(1) 局域网。是在局部地域范围内将计算机、外部设备和网络互联设备连接在一起的网络，可能是一个办公室、一幢大楼、一个学校或一个企业。局域网组建方便，组网成本低，数据传输率高，是目前最实用的网络形式。

(2) 城域网。通常覆盖一个地域相对独立的辖区范围，是扩大了的局域网，是为了满足城域内(如一个学校多个校区、一个企业多个厂区、一家商业机构的多家门店)的各局域网之间的互联而组建的网络。

城域网本质是局域网与局域网之间的联接，随着局域网规模的不断扩大，局域网与城域网的区分已非常困难，城域网的概念将逐步淡化。

(3) 广域网。利用公共(或专用)通信系统将多个局域网(或城域网)互联在一起，实现远程用户之间信息的交换，便构成了广域网。目前广泛使用的国际互联网络(Internet)便是广域网的典型。

1.3.2 按网络的拓扑结构分类

计算机网络的物理连接需要网络设备，将网络设备的物理连接方式采用拓扑学的方法抽象为节点与线的几何关系以描述网络形状，这种网络实体间几何关系的描述称为拓

扑结构。网络拓扑结构反映实际网络的本质。常见的网络拓扑结构有总线型、星形、环形、树形等。

1. 总线型拓扑结构

总线型拓扑结构(见图1-6)采用单根传输线作为传输介质,即总线,所有的站点都通过相应的硬件接口直接连接到传输介质。任何一个站点发送的信号都可以沿着总线传播,而且能被其他所有站点接收。

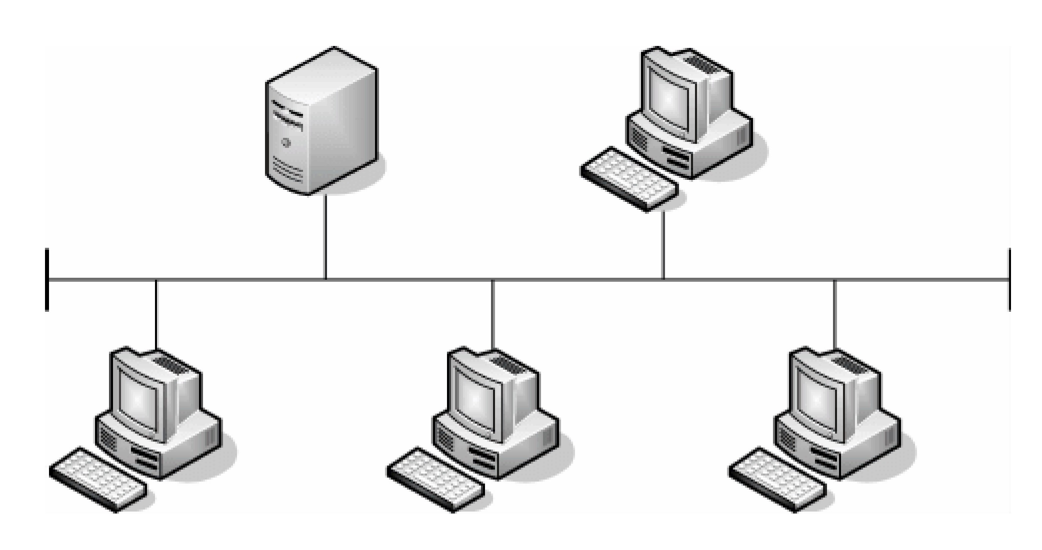


图1-6 总线型拓扑结构

在总线型拓扑结构中,连接的线缆称为总线,终结器是物理终点。当数据在总线上传递时,各站点在接收信息时都进行地址检查,看是否与自己的站点地址相符,若相符则接收该信息,当信号到达网络终点时,终结器将结束信号。

在总线型拓扑结构的网络中,如果接入的计算机数量较多,那么网络速度会明显下降。

总线型拓扑结构有以下优点:

(1) 结构简单,组网容易,网络扩展方便。

(2) 网络布线容易,维护方便。

(3) 多个站点共用一条传输信道,信道利用率高。

(4) 某个站点故障不会引起系统瘫痪。

总线型拓扑结构的缺点如下:

(1) 故障检测需要在各个站点上进行。

(2) 单位时间内两个或两个以上站点传送信息时将产生系统冲突。

(3) 总线故障将造成系统瘫痪。

2. 星形拓扑结构

星形拓扑结构(见图1-7)是指网络中所有节点都连接在一个中央集线设备上,所有数据传送以及信息交换全部通过中央集线设备来实现,是目前应用最广泛的一种网络拓扑结构。

星形拓扑结构的优点如下:

(1) 结构简单,连接方便,管理和维护都相对容易,而且扩展性强。

(2) 网络延迟时间较小,传输误差低。

(3) 在同一网段内支持多种传输介质,除非中心节点故障,否则网络不会轻易瘫痪。

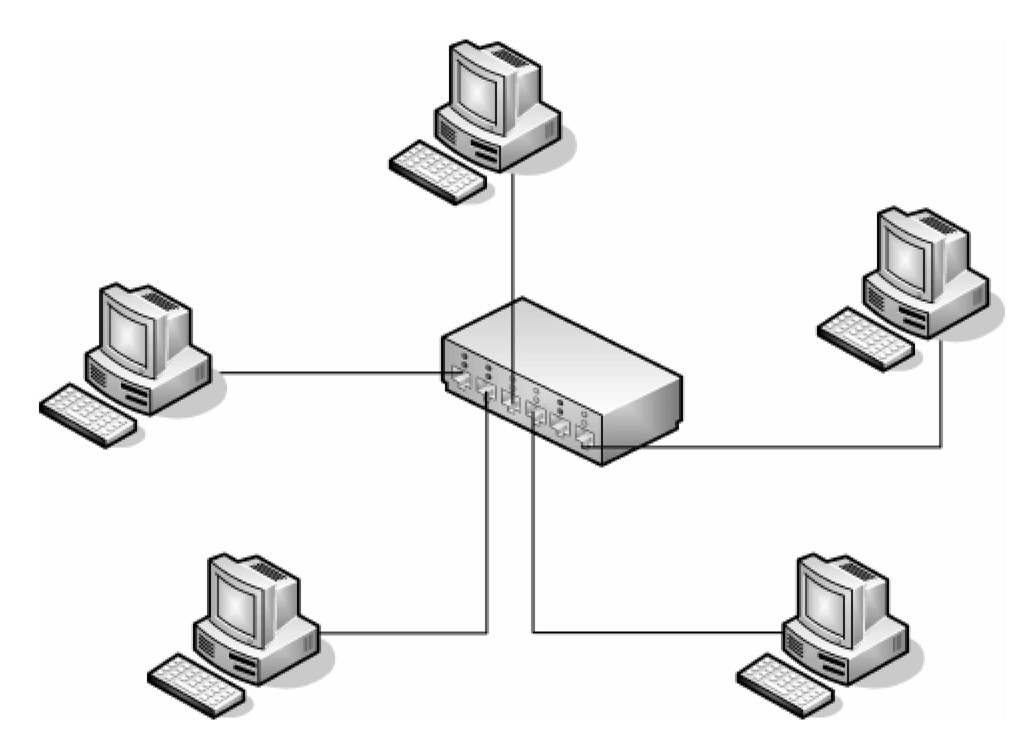


图 1-7　星形拓扑结构

星形拓扑结构的缺点如下：

(1) 安装和维护的费用较高。

(2) 共享资源的能力较差。

(3) 通信线路利用率不高。

(4) 对中心节点要求高，一旦中心节点出现故障，将导致整个网络瘫痪。

3. 环形拓扑结构

环形拓扑结构(见图 1-8)是由连接成封闭回路的网络节点组成的，每一个节点与它左右相邻的节点连接，构成一个环形网络。在环形网络中获得发送信息许可(亦称"令牌")的节点向网络内发送数据，一般情况下传递数据沿逆时针方向穿越网内节点。如果传输数据的目的地址与某节点地址相同时，该节点接收数据。然后，传输数据继续向下一节点传输，直至回到发送信息节点。

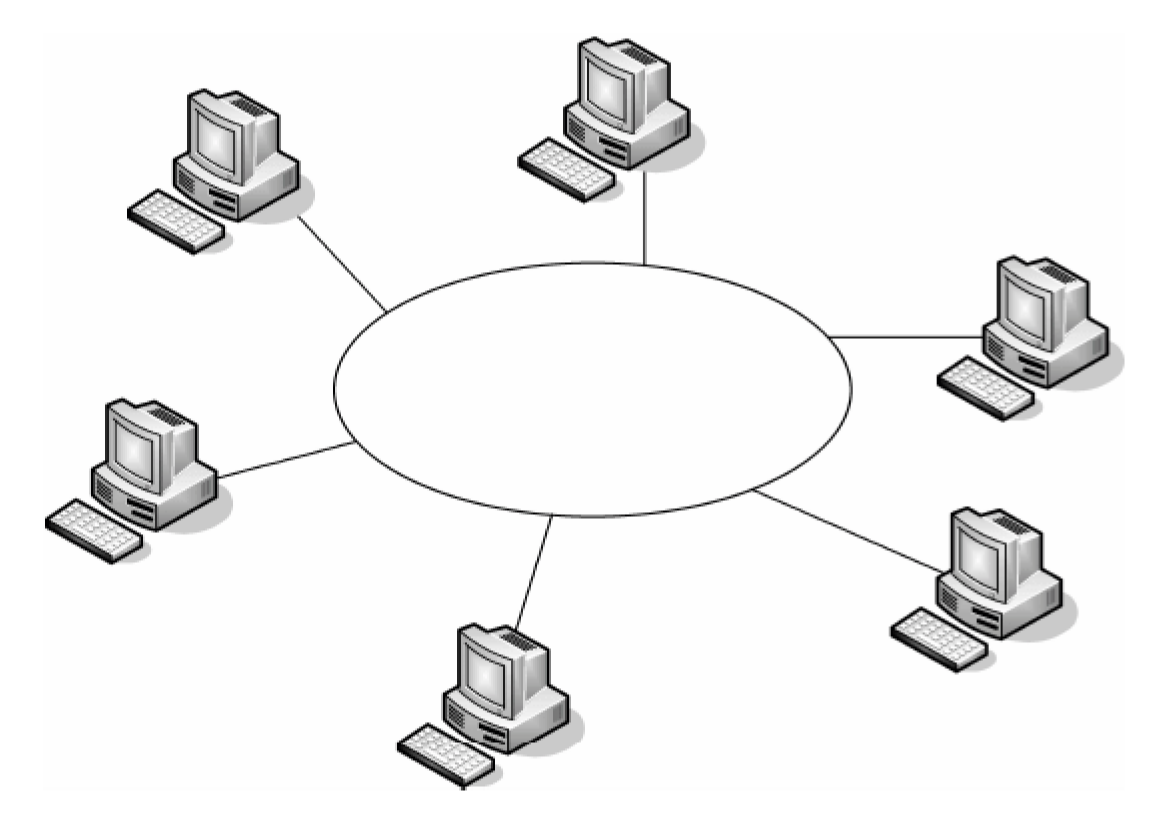


图 1-8　环形拓扑结构

环形拓扑结构的优点如下：

(1) 结构简单，组网成本低。

(2) 数据流在网络中是沿着固定方向流动的，大大简化了路径选择的控制。

(3) 环形网络中的每个节点都拥有相同的访问权,所以在整个网络中数据不会出现冲突。

环形拓扑结构的缺点如下:

(1) 环路封闭,网络扩展比较困难。

(2) 节点增加,传输效率降低。

(3) 单环网络中任一节点出现故障,将影响整个网络。

4. 树形拓扑结构

树形拓扑结构(见图 1-9)从总线型网络拓扑或星拓扑结构扩展而来,由于结构形状像树,因此称为树形拓扑结构。

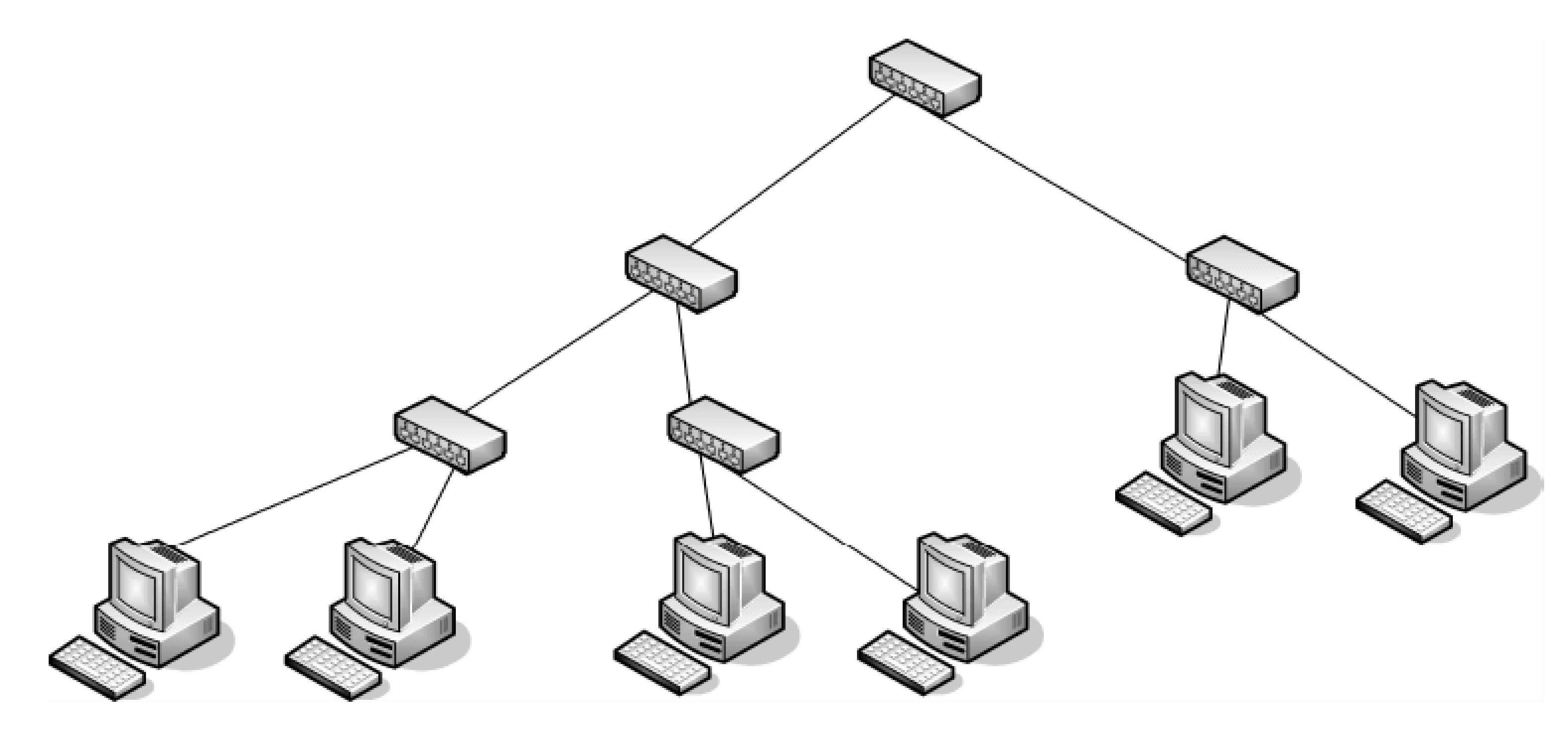


图 1-9 树形拓扑结构

目前,实际应用中以星状树形拓扑结构较多。

树形拓扑结构的优点如下:

(1) 结构简单,成本低。

(2) 网络中任意两个节点之间不产生回路,每个链路都支持双向传输。

(3) 网络中节点扩充方便灵活。

树形拓扑结构的缺点如下:

(1) 拓扑延伸级段有限制。

(2) 根节点产生故障,将影响整个网络系统的正常运行。

1.3.3 按传输技术分类

计算机网络依据所使用的通信传输技术可以分为广播式网络和点到点网络。

(1) 广播式网络。在广播式网络中仅有一条通信信道,该信道由网络上的所有站点共享。在传输信息时,任何一个站点都可以发送数据分组,传到每台计算机上,被其他所有站点接收。这些计算机根据数据包中的目的地址进行判断,如果是发给自己的则接收,否则丢弃。

（2）点到点网络。与广播式网络相反，点到点网络是一条线路连接两个节点或两台计算机，如果两台计算机之间没有直接连接的线路，当一台计算机发送数据分组后，则由它们之间的中间节点对数据分组进行接收、存储和转发直至到达目的站点，这种传输技术称为点到点传输技术，也称为存储转发技术。

1.3.4 其他分类

根据计算机网络应用领域的不同，可将网络分为专用网和公共网两大类。

（1）专用网。这类网络可以是一个局域网的规模，也可以是一个城域网乃至广域网的规模。然而这类网络通常不对社会公众开放，即使开放也有很大的限度，它仅仅是一个企业或企业集团或一个行业内部应用的网络系统。因此这类网络又有很多其他的称呼，如企业网、银行网、校园网等。现在的计算机网络中，专用网也往往是互联网中的一个组成部分。

（2）公用网。顾名思义，公用网的应用领域是对全社会公众开放的，如商业广告、列车/航班时刻查询等各种公开信息便是用这类网络发布的。

根据计算机网络通信介质的不同，可将网络分为有线网和无线网两大类。

（1）使用同轴电缆、双绞线以及光纤等有线介质实现通信的网络称为有线网。

（2）使用卫星、红外线以及微波等无线介质实现通信的网络称为无线网。

1.4 本章小结

计算机网络是现代通信技术与计算机技术快速发展、相互促进、高度融合的产物，计算机网络发展经历了简单到复杂、从低级到高级、从地区到全球的发展过程。按照通信技术和计算机技术结合方式的不同，计算机网络经历了终端式计算机网络、通信中心式计算机网络、体系结构标准化计算机网络和互联高速计算机网络 4 个典型的发展阶段。

计算机网络是指把地理位置不同、系统功能独立的若干台计算机通过通信设备和线路连接起来，借助网络软件，实现网络数据通信和资源共享。因此，计算机网络一般按功能划分为两个主要组成部分：负责数据处理业务，承担网络资源提供与服务的资源子网；负责数据传输与交换控制，提供网络通信功能的通信子网。

计算机网络可以从不同角度进行分类。计算机网络按其覆盖的地理范围分类是最常用的分类方法。按照网络覆盖的地理范围的大小，可以把计算机网络划分为局域网（LAN）、城域网（MAN）和广域网（WAN）3 种类型.计算机网络的物理连接需要网络设备，将网络设备物理连接方式采用拓扑学的方法抽象为节点与线的几何关系以描述网络形状，这种网络实体间几何关系的描述称为拓扑结构。网络拓扑结构反映实际网络的本质。按网络拓扑结构划分计算机网络，常见有总线型、星形、环形和树形等。

综合训练

一、理论题

1. 选择题

(1) 计算机网络的发展经历了 4 个阶段，其中第 4 阶段是以(　　)为核心的网络时代。

A. 局域网　　B. 面向终端式网络
C. Internet　　D. 分组交换网

(2) 在计算机网络中负责执行通信控制功能的设备称为(　　)。

A. 通信线路　　B. 终端
C. 主计算机　　D. 通信控制处理机

(3) 计算机网络中，资源子网承担面向应用的数据处理和网络(　　)，它由各种硬件和软件组成。

A. 资源共享　　B. 分布处理　　C. 终端输出　　D. 通信控制

(4) 计算机网络分为广域网、城域网和局域网，其划分的主要依据是网络的(　　)。

A. 拓扑结构　　B. 控制方式　　C. 作用范围　　D. 传输介质

(5) 计算机网络拓扑通过网中节点与通信线路之间的几何关系反映出网络中各实体之间的(　　)关系。

A. 结构　　B. 层次　　C. 服务　　D. 逻辑

2. 填空题

(1) 计算机网络发展的 4 个阶段是终端式、通信中心式、________和________。

(2) 计算机网络是________技术与________技术结合的产物。

(3) 常见的计算机网络拓扑结构为________、________、________和________。

(4) 计算机网络依据所使用的通信传输技术可以分为________和________网络。

(5) 根据计算机网络通信介质的不同，可将网络分为________和________两大类。

3. 简答题

(1) 计算机网络的发展经过哪几个阶段？每个阶段各有什么特点？

(2) 什么是计算机网络？计算机网络的主要功能是什么？

(3) 计算机网络按功能分为哪些子网？各个子网都包括哪些设备？各有什么特点？

(4) 计算机网络是如何分类的？

(5) 计算机网络的拓扑结构有哪些？它们各有什么优缺点？

二、实践题

1. 家庭 ADSL 接入 Internet 拓扑绘制

参考步骤如下：

（1）打开 Visio（见图 1-10），选择“文件”→“新建”命令。



图 1-10 Visio 界面

（2）在“模板类别”中选择“网络图”，再双击“详细网络图”，见图 1-11。

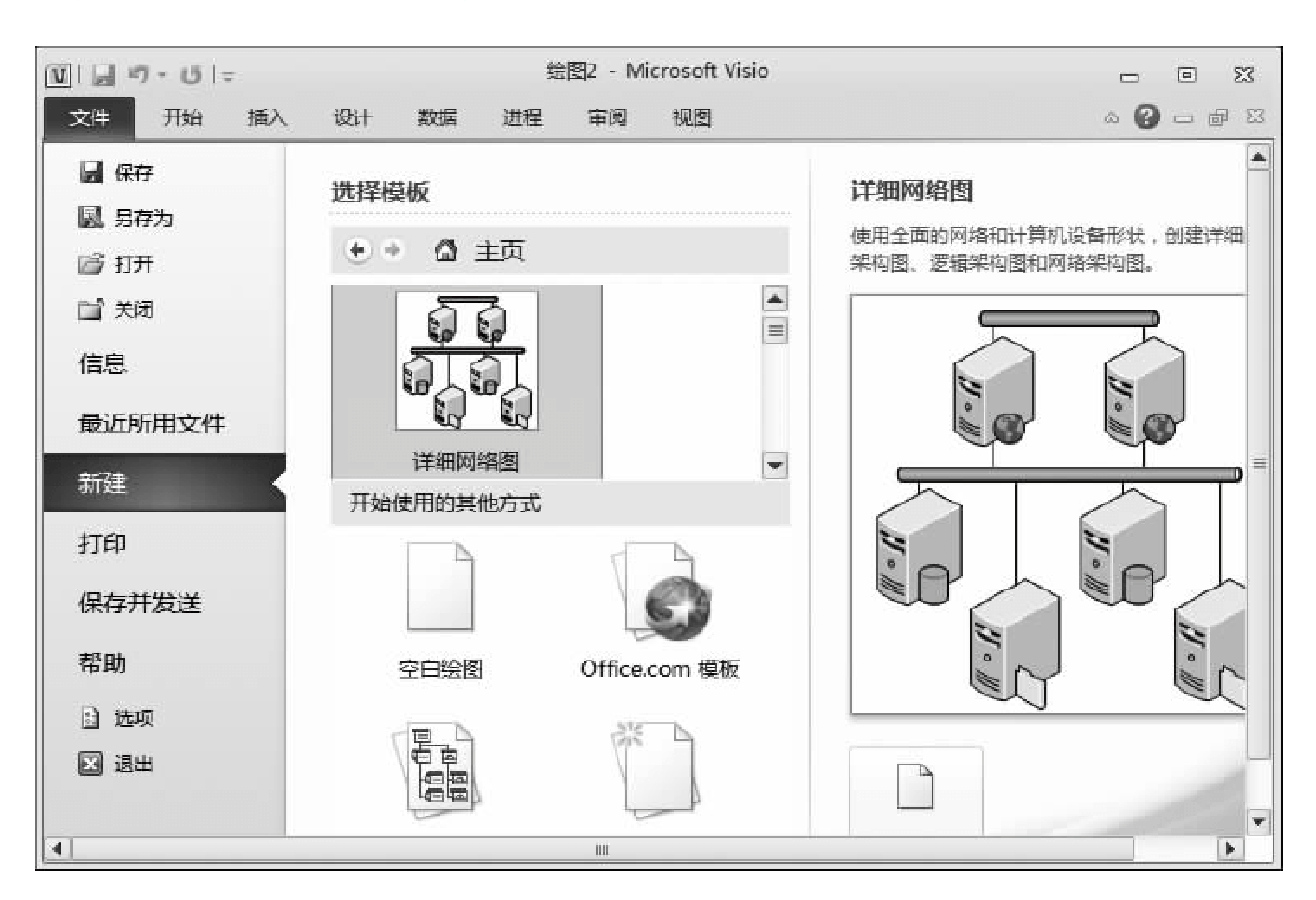


图 1-11 选择绘制图形类别

（3）添加绘图形状，见图 1-12。

（4）绘制“家庭 ADSL 上网拓扑结构”，见图 1-13。

2. 绘制实验室网络拓扑结构

认真查看实验室的网络连接情况，绘制出实验室网络拓扑结构。



图 1-12　添加绘图形状

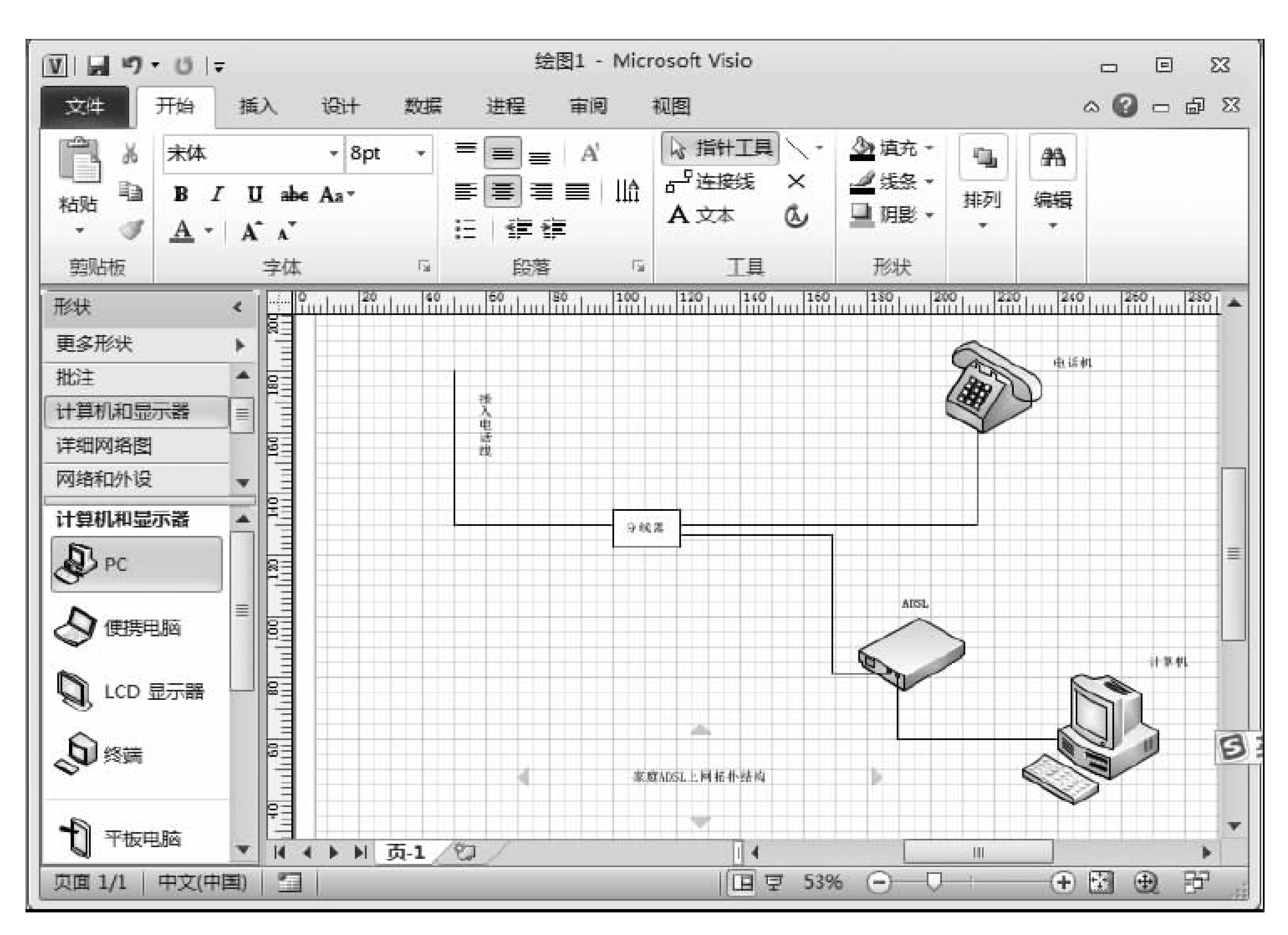


图 1-13　ADSL 上网拓扑结构

第 2 章　计算机网络体系结构与协议

本章主要内容

- 计算机网络体系结构的基本概念
- 开放系统互连参考模型 OSI/RM
- 互联网应用模型 TCP/IP
- IP 地址和子网掩码

计算机网络体系结构是为了完成计算机间的通信合作，把计算机网络互连的功能划分成有明确定义的层次，并规定了同层次进程通信的协议及相邻之间的接口与服务。为了实现不同厂家生产的计算机系统之间以及不同网络之间的数据通信，国际标准化组织(ISO)制定了开放系统互连参考模型，即 OSI/RM。

TCP/IP 是一组用于实现网络互联的通信协议。Internet(因特网)网络体系结构以TCP/IP 为核心。子网掩码是与 IP 地址配合使用的技术，主要解决了两个问题，一是快速区分 IP 地址中的网络标识与主机标识，二是解决大型 IP 网络划分子网的问题。

2.1　计算机网络层次结构

计算机网络体系是一个非常复杂的结构，为使网络结构逻辑清晰，国际标准化组织采用层次化结构来定义计算机网络系统的组成与系统实现。它将一个网络系统分成若干层次，并且规定了每个层次应该实现的功能及应该向上层提供的服务，同时规定了两个系统的各个层次实体之间进行通信时应该遵守的协议。

2.1.1　网络体系结构的发展与定义

计算机网络体系结构是用结构化、层次化方法去分析计算机网络这个复杂事物，以达到从抽象角度去把握和理解计算机网络的目的。

1974 年美国 IBM 公司在网络实践中总结出世界上第一个网络体系结构——系统网络体系结构(System Network Architecture，SNA)。凡是遵循 SNA 的网络设备都具有互连性，网络体系结构采用分层结构的思想，具有开创意义。

网络体系结构(network architecture)是计算机网络的分层、各层协议、功能和层间接口的集合。不同的计算机网络具有不同的体系结构，其层的数量、各层的名称、内容和功能及各相邻层之间的接口都不一样。然而，在任何网络中，每一层都是为了向它相邻的上层提供一定的服务而设置的，而且每一层都对上层屏蔽实现协议的具体细节，这样网络体系结构就能做到与具体的物理实现无关，尽管连接到网络中的主机型号及性能各不相同，

但只要它们共同遵守相同的协议，就可以实现互通信和互操作。

所谓层次结构，就是把一个复杂的系统问题分解成多个层次分明的局部问题，并规定每一层次所必须完成的任务。层次结构提供了一种按层次来观察网络的方法，它描述了网络中任意两个节点间的逻辑连接和信息传输。

网络体系结构是一个抽象的概念，因为它不涉及具体的实现细节，只是说明网络体系结构必须包括的信息，以便网络设计者能为每一层编写符合相应协议的程序，而不必考虑具体的硬件实现方法。

2.1.2 网络协议

在计算机网络中，相互通信的双方处在不同的地域，双方相互通信时需要交换信息来协调它们的动作，以达到同步。而信息交换必须按照预先约定好的规则进行，在计算机网络中通信双方都遵守的规则称为网络协议。

1. 网络协议特性

(1) 层次性。由于网络体系结构是有层次的，所以网络协议也分成多个层次，每个分层还可以进一步分成若干个子层次。

(2) 可靠性。如果网络协议不可靠，就会造成通信混乱和中断。

(3) 有效性。只有网络协议有效，才能实现系统内的资源共享。

2. 网络协议的 3 个要素

(1) 语法。语法用于规定将若干个协议元素和数据组合在一起，以表达一个更完整的内容时所应遵循的格式，即是对所表达的内容的数据结构形式的一种规定。它涉及数据及控制信息的格式、编码及信号电平等。

(2) 语义。协议的语义是指对构成协议的协议元素含义的解释，以完成规定的控制操作，即解决如何进行操作或如何作出应答的问题。

(3) 时序。时序规定了事件的执行顺序，即通信过程中的应答关系和状态变化关系。时序涉及速度匹配与排序等问题。

2.1.3 网络体系结构中的基本概念

以下是一些用于描述网络体系结构的基本概念。

(1) 层。如前所述，计算机网络是一个复杂系统，必须从逻辑功能上将这样一个复杂系统划分成多个层次，实现模块化任务处理，各层处理自己所承担的任务。

(2) 实体。实体是通信时能发送和接收信息的任何软硬件设施。网络分层结构中，每一层都由一些实体组成，这些实体抽象地表示了通信时的软件或硬件。

(3) 服务。在计算机网络中，服务(service)是一个纵向概念，是指第 N 层的所有实体为第 $N+1$ 层的所有实体提供的功能集合，由于第 N 层与第 $N+1$ 层之间的单向依赖关

系，所以服务具有单向性（即从下向上），也就是说，上层实体可以调用下层实体，下层实体只能返回结果。一般将下层实体提供给上层实体调用形式参数并且返回结果的地方称为服务访问点（Service Access Point，SAP）。

（4）服务原语（service primitive）。是一种起始动作信息，它既可由服务用户发出（如Request，Response），也可由服务提供者发出（如 Indication，Confirm）。服务原语供用户实体访问该服务或者向用户实体报告某事件的发生。也就是说，某一层的实体通过规范化语言来要求另一实体提供什么服务，或是可以为另一实体提供什么服务。服务原语可以分为 4 种类型，如表 2-1 所示。

表 2-1　服务原语

原　　语	功　　能
请求（Request）	使服务的用户能从服务提供者那里请求一定的服务（如建立连接、发送数据、报告状态等）
指示（Indication）	使服务提供者能向服务的用户提示某种状态（如连接提示、输入数据、拆除连接等）
响应（Response）	使服务的用户能响应先前的指示原语（如接受连接等）
确认（Confirm）	使服务提供者能报告先前的请求原语请求成功与否

（5）数据单元。为了实现某些功能，层与层之间、实体与实体之间都需要传递一些数据，通常将传递的数据的每一个单位叫做数据单元（Data Unit，DU）。

（6）协议数据单元。通常将不同计算机系统的对等层实体之间，为实现同层协议所交换的信息单元称为协议数据单元（Protocol Data Unit，PDU）。

（7）服务数据单元。第 N 层要求第 $N-1$ 层提供服务时所要传递的逻辑数据单元称为服务数据单元（Service Data Unit，SDU）。也就是说，服务数据单元是指下层实体给上层实体返回结果的集合。

（8）接口数据单元。在同一系统的相邻两层实体的交互中，传递层间接口的信息单元称为接口数据单元（Interface Data Unit，IDU）。

2.2　开放系统互连参考模型

1984 年，国际标准化组织（ISO）正式公布了一个网络体系结构国际标准，称为开放系统互连参考模型（OSI/RM）。这里的“开放”是指任何两个遵守 OSI/RM 的系统都可以进行互连。当一个系统能按 OSI/RM 与另一个系统进行通信时，就称该系统为开放系统。

2.2.1　层次结构

在 OSI 参考模型（见图 2-1）中，将整个通信功能划分为 7 个层次。每一层的目的是向相邻的上一层提供服务，并且屏蔽服务实现的细节。模型设计成多层，像是在与另一台

计算机的对等层通信。实际上，通信是在同一计算机的相邻层之间进行的。每一层都按照一组协议来实现某些网络的功能。7 个层次之间的问题相对独立，而且易于分开解决，也无须过多依赖于外部信息。7 个层次自下而上分布，并具有不同的功能。

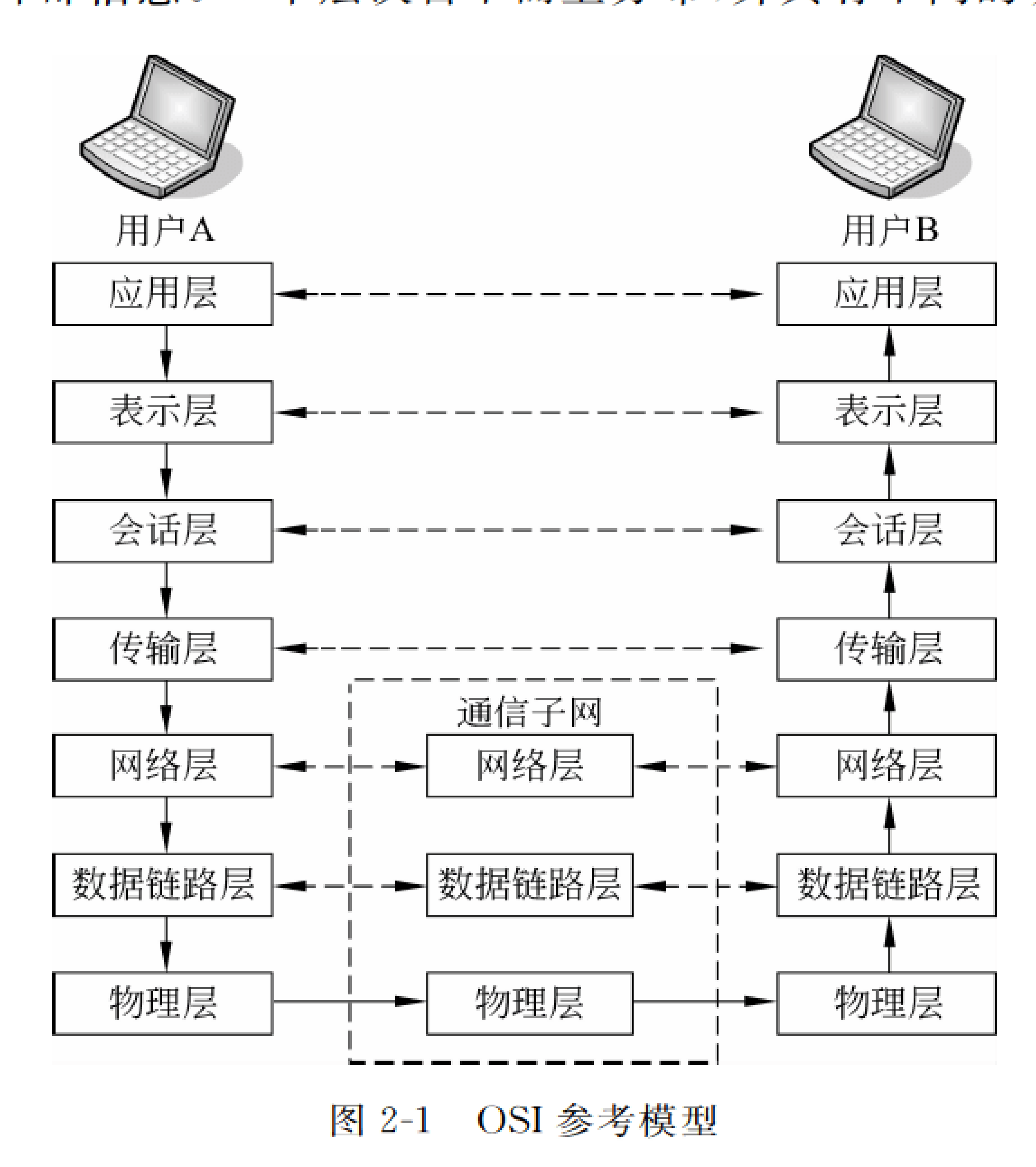


图 2-1 OSI 参考模型

2.2.2 物理层

1. 物理层的概念

物理层(physical layer)位于 OSI 参考模型的底层，它建立在物理通信介质的基础之上，作为系统和通信介质的接口，用来实现数据链路实体之间透明的比特流传输。物理层以比特流的方式传送来自数据链路层的数据，而不必考虑数据的含义或格式，物理层的信息传输单元是比特；同样，它接收数据后，也不加分析，直接传给数据链路层。物理层协议关心的典型问题是使用什么样的物理信号来表示数据 1 和 0；一位持续的时间多长；数据传输是否可同时在两个方向上进行；最初的连接如何建立和完成；通信后连接如何终止；物理接口 (插头和插座)有多少针及各针的用处。

物理层的设计主要涉及物理层接口的机械、电气、功能和过程特性，以及物理层接口连接的传输介质等问题。

2. 物理层的功能

为了实现数据链路实体之间比特流的透明传输，物理层具有以下功能。

(1) 物理连接的建立与拆除。当数据链路层请求在两个数据链路实体之间建立物理连接时，物理层应立即为它们建立相应的物理连接。若两个数据链路实体之间有若干中

继数据链路实体时,物理层还应对这些中继数据链路实体进行互连,以建立一条有效的物理连接。当不再需要物理连接时,应由物理层立即拆除它们。

(2)物理层服务数据单元传输。物理层既可以采取同步传输方式来传输物理层服务数据单元,也可以采取异步传输方式来传输物理层服务数据单元。

(3)物理层管理。物理层涉及本层的某些管理事务,例如功能的激活(发送、接收、异常情况处理)和差错控制等。

3. 物理层的特性

物理层是OSI参考模型中唯一涉及通信介质的一层,它负责提供与通信介质的连接,描述这种连接的机械、电气、功能和规程特性,以建立、维护和释放数据链路实体之间的物理连接。

物理层协议定义了硬件接口的一系列标准,它涉及以下4个特性。

(1)机械特性。主要规定了接口连接器的尺寸、介质芯数与通信安排、连线数量等。常用的连接器有9芯、15芯和25芯等规格。

(2)电气特性。主要规定了每种信号的电平、脉冲宽度、允许的数据传输速率和最大传输距离。

(3)功能特性。规定了接口电路引脚的功能和作用。

(4)规程特性。规定了接口电路信号发出的时序、应答关系和操作过程。例如,规定了怎样建立和拆除物理层连接、是全双工还是半双工等内容。

2.2.3 数据链路层

1. 数据链路层的概念

数据链路层(data link layer)的主要用途是在相邻网络实体之间建立、维持和释放数据链路连接,并且传输数据链路服务数据单元(即frame,一般称为数据帧或帧)。换言之,数据链路层的主要职责是控制相邻系统之间的物理链路,它在物理层信息传送的基础上,在相邻节点之间传送被称为帧的数据信息,因此数据链路层传输的数据单元是帧。

由于种种原因,数据传输过程中可能会出现差错,数据链路层需要进行数据检错和纠错,从而向网络层提供无差错的透明传输。

数据链路层是任何网络必须具有的层次,数据链路层在网络实体之间建立、维持和释放数据链路,提供传输数据链路服务数据单元所需要的功能和过程管理。数据链路连接建立在物理连接基础上,在物理连接已经建立时,一般可保持较长时间不变。每次通信前后,双方相互联系,以确认一次通信的开始和结束,也就是建立数据链路连接和拆除数据链路连接。

发送方和接收方主要是通过帧数据单元进行操作,在相邻节点之间建立起可靠的数据链路。就是说,发送方先把数据封装成一个一个的帧,然后按照顺序发送给接收方。在发送过程中有可能出错,所以接收方必须采取一定方法对接收到的数据进行校验,一旦接

收方发现发送方发送的某些帧数据单元有错，就必须自己改正或者通知发送方，要求发送方再发送一次。因此，可靠的数据链路的建立是通过帧的组装、帧的校验和帧的重发来实现的。在此过程中，帧的校验显得非常重要，如果接收方不能有效检查出数据在传输过程中出现了错误，则说明数据链路是不可靠的，因此，数据链路层采用多种校验技术来保证通信的准确性。

2. 数据链路层提供的功能和服务

数据链路层最基本的服务，是将数据传输源主机从网络层发来的数据可靠地传输到相邻节点的目标主机的网络层。为了达到这一目的，数据链路层必须具备如下所述的一系列功能。

(1) 数据链路管理功能。在链路两端的节点进行通信之前，首先确认对方已处于就绪状态，并且交换一些必要信息来初始化，然后才能建立连接，在传输过程中则要维持该连接。传输完毕后，释放连接。如果出现差错，则要重新初始化，重新自动建立连接。数据链路层连接的建立、维持和释放称为链路管理。

(2) 差错控制功能。通信系统必须具备检测差错的能力，如果发现差错，就需要采取措施加以纠正，使差错控制在允许范围内，这就是差错控制。差错控制是数据链路层的主要功能之一。接收方通过对差错编码进行检查，就可以判定某一帧在传输过程中是否发生了差错。一旦发现差错，可以采用反馈重发来加以纠正。这就要求接收方接收完一帧以后，向发送方反馈一个接收是否正确的信息，发送方据此做出是否需要重新发送的决定。发送方仅当收到接收方正确接收的反馈信号后，才能认为该帧已经正确发送完毕，否则需要重新发送，直到正确为止。

(3) 相邻节点之间的流量控制。由于收发双方各自使用的设备的工作速率和缓冲存储空间的差异，很可能会出现发送方的发送能力大于接收方的接收能力这种现象。此时，如果不对发送方的发送速率或信息流量进行必要控制，接收方来不及接收的帧将被后面不断发送来的帧“淹没”，造成帧丢失现象。由此可见，流量控制实际上是对发送方的数据流量进行控制，使其发送速率不超过接收的速率。

需要说明的是，流量控制并不是数据链路层独有的功能，许多高层协议也提供流量控制功能，只不过流量控制的对象不同而已。

3. 数据链路层的主要协议

数据链路层协议通常称为通信规程，包括异步控制协议和同步控制协议两大类，其中异步控制协议由于信道利用率较低，一般用于数据速率较低的场合。在数据链路层同步控制协议中，面向字符的通信规程和面向位(比特)的通信规程是具有代表性的两种同步控制协议，分别介绍如下。

1) 面向字符的通信规程

该规程的代表是 BSC 协议，传送的信息单位是帧。这类规程一般利用若干个控制字符控制报文的传输。报文通常由报头(header，也译为标题)和正文(body)两部分组成。其中，报头含有报文名称、源地址、目的地址和发送日期等用于传输控制的字段，报头的作

用就相当于日常生活邮寄信件的信封，在信封上必须写明收信人是谁、谁寄的信等控制信息。正文相当于信件内容，是目的节点实际接收的数据内容，当然正文必须有开始标志和结束标志。所以，这种通信规程主要是对报文的格式进行规定。当目的站收到报文时，若正确，则向源站发送确认的控制字符；若有错，则发回拒绝接收的控制字符。

典型的报文格式如表2-2所示。

表2-2　面向字符的报文格式

SOH	报头	STX	报文文本	ETX/ETB	校验

BSC协议传输控制字符的功能如下：

SOH(Start of Head)：序始，用于表示报文的报头(header)或标题信息的开始。

STX(Start of Text)：文始，标志报头的结束和报文文本(body)的开始。

ETX(End of Text)：文终，标志报文文本的结束。

EOT(End of Transmission)：送毕，用以表示一个或多个文本的结束，并拆除链路。

ENQ(Enquire)：询问，用以请求远程站给出响应，响应可能包括站的身份或状态。

ACK(Acknowledge)：确认，由接收方发出，作为对正确接收到报文的响应。

DLE(Data Link Escape)：转义，用以修改紧跟其后的有限个字符的意义。

NAK(Negative Acknowledge)：否认，由接收方发出，作为对未正确接收到报文的响应。

SYN(Synchronous)：同步字符，在同步协议中，用以实现节点之间的字符同步，或用于在无数据传输时保持该同步。

ETB(End of Transmission Block)：块终或组终，用以表示当报文分成多个数据块时一个数据块的结束。

BSC协议将在链路上传输的信息分为数据和监控报文两类。监控报文又可分为正向监控和反向监控两种。每一种报文中至少包括一个传输控制字符，用以确定报文中信息的性质或实现某种控制作用。

2）面向位的通信规程

面向位的通信规程的典型例子是ISO制定的高级数据链路控制协议(High-level Data Link Control，HDLC)。该规程的信息传送单位也是帧，但用来填充控制信息的是比特。帧进一步细分为数据帧和控制帧，并且这些位流中都用一个明显的8位或者16位来划分边界(见表2-3)，故称为面向位的通信规程。位流用帧标志来划分帧边界，帧标志也可以用做同步字符。

表2-3　面向位的报文格式

标志(F)	地址(A)	控制(C)	信息(I)	帧校验(FCS)	标志(F)
01111110	8位	8位	任意长	16位	01111110

HDLC协议传输控制字符的功能如下。

标志(F)：HDLC指定采用01111110为标志序列，称为F标志。要求所有的帧必须

以F标志开始和结束。接收设备不断地搜寻F标志,以实现帧同步,从而保证接收部分对后续字段的正确识别。

地址(A):地址字段,内容由操作方式决定。在使用不平衡方式传送数据时,地址字段总是写入从站的地址;在使用平衡方式时,地址字段总是写入主站的地址。地址字段的长度一般为8位,最多可以表示256个站的地址。

在链路上用于控制目的的站称为主站,其他的受主站控制的站称为从站。主站负责对数据流进行组织,并且对链路上的差错实施恢复。由主站发往从站的帧称为命令帧,而由从站返回主站的帧称为响应帧。

控制(C):控制字段用来表示帧类型、帧编号以及命令、响应等。HDLC帧分为3种类型:信息帧、监控帧和无编号帧。另外控制字段也允许扩展。

信息(I):信息字段内包含了用户的数据信息和来自上层的各种控制信息。该字段可以是任意长度的比特序列,在实际应用中,其长度由收发站的缓冲器的大小和线路的差错情况决定,但必须是8位的整数倍。

帧校验(FCS):帧校验序列用于对帧进行循环冗余校验,其校验范围是从地址字段的第1位到信息字段的最后一位的序列。

面向位的通信规程有许多优点。首先,HDLC在正文字段没有位数限制,可以传送字符数据或者其他数据。面向字符的通信规程只能传输8位的字符数据。其次,面向字符的规程规定了一些控制字符,但对接收端来说不好判断。而HDLC使用了唯一标志(01111110,即7EH),其效率和透明性都较好。

2.2.4 网络层

网络层(Net work Layer)是通信子网与资源子网之间的接口,是高低层之间的分界。网络层的主要用途,是为了实现网络中主机间的通信而建立、维护、终止网络连接,并且通过网络连接来交换网络服务数据单元(即packet,一般称为数据包或报文分组)。两个端系统的传输实体之间要进行通信,只需要将要交换的数据交给它们的网络层即可实现。

网络层就是负责将数据从源主机可靠地传输到目的主机。网络层主要涉及计算机网络中的通信子网,处理通信子网中节点与节点之间的关系。

1. 网络层的功能

网络层的主要功能是支持网络连接的实现。它包括点到点结构的网络连接及由具有不同特性的子网所支持的网络连接等。网络层的具体功能如下所述。

(1) 建立和拆除网络连接。本功能是指利用数据链路层提供的数据链路连接构成传输实体间的网络连接。网络连接同样也可由若干通信子网以串联形式来构成。这些互连的子网可具有相同或者不同的服务能力,子网连接的两端可以采用不同的子网协议。

(2) 路径选择。路径选择是网络层中一个非常重要的功能,在广域网中更是如此。路径选择一般称为路由(routing),是指网络中的节点根据网络的当前情况在很多条路径中选择一条耗时最短的路径来传输数据。当然,这种选择要求节点先根据复杂的路径选

择算法来对网络当前情况做出测量，然后再进行比较和选择。路由选择可比喻为在某个大城市的复杂公路交通体系中为车辆选择行进路线，因为路上的车流量和路况都是随时变化的，而我们必须为车辆动态地选择一条最合适的线路，让车辆能够安全、可靠、高效地到达目的地。

（3）对数据进行分段和组装。为了提高传输效率，当通信子网中的某一节点收到某个数据单元以后，要将该数据单元向通信子网中的下一个节点发送。如果这个数据单元太长的话，则对方很可能没有相应的接收能力。因此，该节点不能直接将大的数据单元转发出去，而是必须将该数据单元进行分组。反过来，当接收的单元较小时，就要将数据单元进行组装，然后再转发到通信子网中的下一个节点。

（4）传输和流量控制。网络中的数据在进行传输时，有时会发生网络拥塞现象。为了避免出现网络拥塞，网络层必须对通信子网中的数据流量进行有效控制，使网络流动顺畅，这是网络层的功能之一。

（5）差错的检测和恢复。前面已经介绍过，数据链路层主要负责差错检测。但是，网络层有时也负责对网络中的数据进行检测和恢复。

2. 网络层提供的主要服务

在OSI/RM中，网络层提供两种类型的网络服务：数据报（data-gram）服务，见图2-2；虚电路（Virtual Circuit，VC）服务，见图2-3。

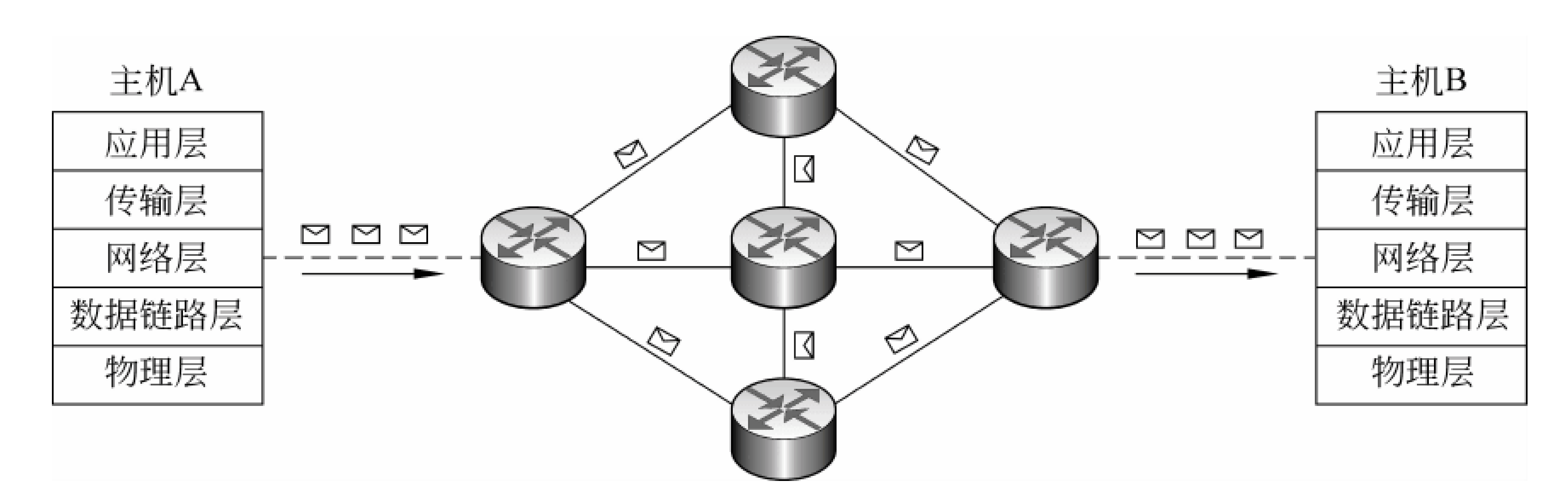


图2-2　数据报服务

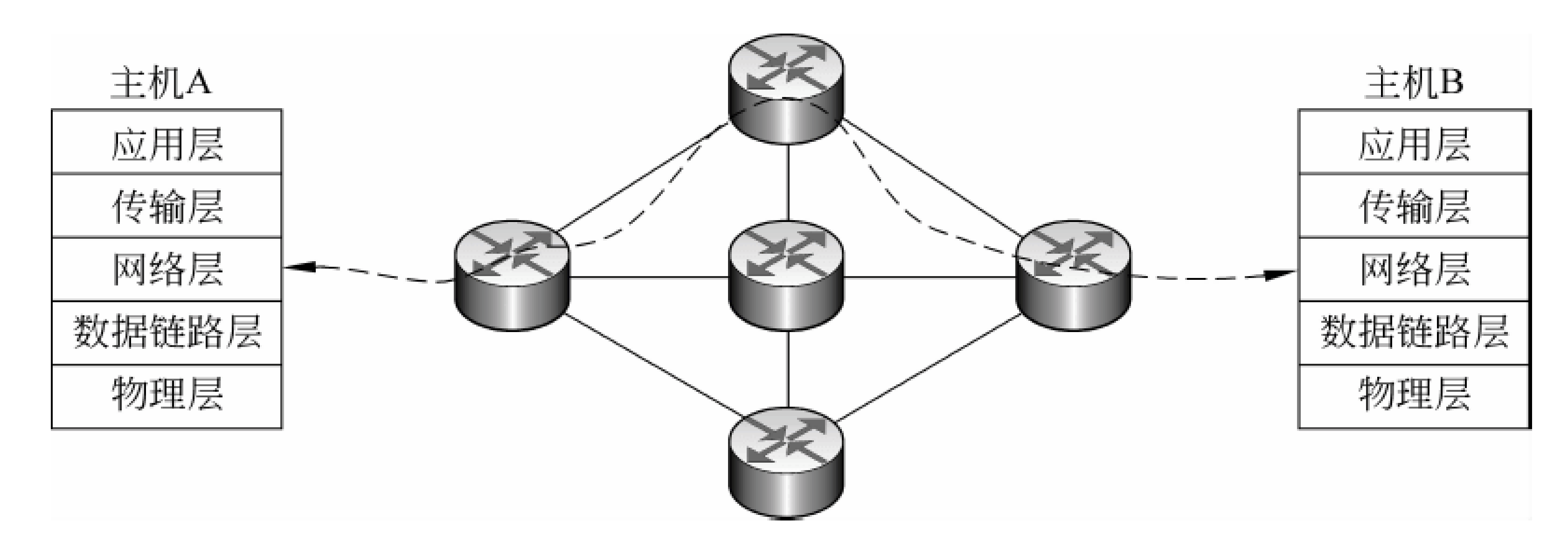


图2-3　虚电路服务

1）数据报服务

在数据报传输方式中，网络层负责从传输层接收报文并拆分为报文分组，将每一个分

组作为一个独立的信息单位进行传送，在传输过程中不考虑它与前面已发出的数据报的顺序关系。数据报每经过一个中间节点，都要根据当时的网络情况和一定的路径选择算法来选择一条最佳路径。在数据传输过程中，很可能出现后传输的数据报先到达这种情况，这与发送电报和信件的传输方式相类似。

2）虚电路服务

虚电路服务是网络层向传输层提供的，能使所有分组按顺序到达目的端系统的一种可靠的数据传送方式。进行数据交换的两个端系统之间存在着一条为它们服务的虚电路。所谓虚电路，是指两个端系统之间的一条虚拟链路，这就像两个电话机之间进行通话时，需要通过一系列命令来建立一条链路。链路建立起来以后，要传送的数据包就会沿着该逻辑链路向前传送。这个链路可能需要几个中间设备的支持。当通信完毕后，该虚电路可能还会存在，也可能被拆除。为了建立端系统之间的虚电路，源端系统的传输层首先向网络层发出连接请求，网络层则通过虚电路网络访问协议向网络节点发出呼叫分组。在目的端，网络节点向端系统的网络层传送呼叫分组，网络层再向传输层发出连接指示。最后，接收方的传输层向发送方发回连接响应，从而建立起虚电路。此后，两个端系统之间就可以传送数据。数据由网络层拆成若干分组传送给通信子网，由通信子网将分组传送到数据接收方。虚电路服务如图 2-3 所示。

数据报服务适合传送数据量较小的数据，而且对速度的要求比对质量的要求更高。虚电路刚好相反，它比较适合传送数据量较大的数据，而且对传输过程中的可靠性要求较高。虚电路服务是网络层向传输层提供的一种服务，也是通信子网端系统提供的一种网络服务。

3）永久虚电路和暂时虚电路

所谓永久虚电路，是指两个主机之间建立的一条永久性连接。由于这两个主机之间很可能经常传输很多数据，所以需要建立一条永久虚电路，从而不需要每次通信时都执行建立和拆除虚电路的操作。暂时虚电路就是一般意义上的虚电路，即根据主机的请求而建立的逻辑连接，传输完数据以后就进行拆除。

数据报服务和虚电路服务的简单比较如表 2-4 所示。

表 2-4　数据报与虚电路服务的比较

比 较 项 目	数据报服务	虚电路服务
目的主机地址	每个分组都需要	建立连接的第一个分组
初始化设置	不需要	需要
分组顺序	发送与接收顺序可以不一致	发送与接收顺序相一致
差错控制	由主机负责	由通信子网负责
流量控制	网络层不负责	由通信子网负责
连接的建立和拆除	需要	不需要
适用情况	传送量小、速度要求高的数据包	传送量大、可靠性要求高的数据包

2.2.5 传输层

传输层在计算机网络中总体负责传输服务数据单元(即 segment,一般称为报文)的数据传输和数据控制,为两个端系统的会话层建立、维护和取消传输连接,负责端到端的可靠数据传输。

传输层下面的3层属于通信子网,完成有关的通信处理,向传输层提供网络服务;传输层上面的3层完成面向数据处理的功能,为用户提供与网络之间的接口。由此可见,传输层在OSI参考模型中起到承上启下的作用,是整个网络体系结构的关键。

1. 传输层提供的服务

传输层的主要任务是在优化网络层提供的服务的基础上,在源主机与目的主机之间提供可靠的透明数据传输,使高层服务用户在相互通信时不必考虑通信子网的实现细节。事实上,设计传输层的初衷就是在网络层的基础上再增添一个软件层,使之能够屏蔽各类通信子网的差异,向用户的应用进程提供一个能够满足其要求的服务,并且具有一个不变的通用传输层接口。这样,用户进程只需要了解该接口,就可以方便地在网络上使用各种网络资源和进行网络通信。传输层通常提供以下两种服务。

(1) 面向连接服务。面向连接服务就是在数据交换之前必须先建立连接,当数据交换结束后则应该终止这个连接。面向连接服务比较适合于在一定期间内要向同一目的地连续发送许多报文的情况。若实体间经常进行频繁通信,则请求网络层建立永久虚电路,这样可免除每次通信时连接建立和连接释放这两个过程。

(2) 无连接服务。在无连接服务的情况下,两个实体之间的通信不需要先建立好一个连接,因此其下层的有关资源不需要事先进行预留,这些资源是在数据传输时动态地进行分配的。无连接服务不需要通信的两个实体同时处于激活状态,当发送端的实体正在进行发送时,它必须是激活的,但这时接收端的实体并不一定要激活。只有当接收端的实体正在进行接收时,它才必须是激活的。

无连接服务的优点是灵活方便和比较迅速,但无连接服务不能防止数据包的丢失、重复或失序。当采用无连接服务时,由于每个数据包都必须提供完整的源地址与目的站地址,因此通信开销比较大。

2. 传输层的主要功能

传输层主要实现以下功能。

(1) 将传输层的地址映射到网络地址。要将传输层服务数据单元从一个传输层实体传送到另一主机上的传输层实体,传输层必须将传输层的地址映射到网络地址。OSI参考模型规定,一个传输层实体可以为多个会话层实体服务。因此,一个网络地址可以与多个传输层地址相连接。传输层的使用者是用户进程,用户进程要想实现通信,则必须调用传输层的某一个实体,这样才能通过该实体建立起一条传输通路。因此,从传输层提供给应用层并且供其调用的接口或者参数就是所谓的传输层地址。

传输层要将相应的传输层地址与相应的应用层实体对应起来，传输层为了利用网络层，还要在某个传输层地址与网络之间建立一对一或者一对多的对应关系，即所谓的映射。

(2) 多路复用和分割。为有效地利用网络连接，传输层连接与网络连接之间的映像可采用以下3种形式。① 一一对应，一条传输层连接映射为唯一的一条网络连接。②多路复用，利用一条网络连接来支撑多条传输连接，使网络连接得到充分使用，以减少费用。③分割，利用多条网络连接来支撑一条传输连接，以提高传输服务质量，并改善传输的可靠性。

(3) 传输连接的建立与释放。该功能用于为两个会话实体建立传输层的虚拟连接。在此阶段，传输层必须使所要求的服务类型与网络所提供的服务相匹配。这些功能包括：获得一条网络连接，网络连接的多路复用和分割，建立最佳的传输层协议数据单元长度，选择进入数据传输阶段后可供使用的功能，将传输地址映射到网络地址，对传输连接进行识别。

(4) 分段与重新组装。在发送方，传输层的某一实体可以将传输层的服务数据单元分段为多个网络服务数据单元；而在接收时，接收方传输层的某一实体将收到的网络服务数据单元重新组装为传输服务数据单元。

(5) 组合与分解。当用户数据很小时，发送方的某一传输层实体可以将多个传输层服务数据单元组合成一个网络服务数据单元，而后再交给网络层进行处理；接收方的传输层实体将接收到的网络层协议数据单元重新分割为多段传输层服务数据单元，经过处理后交给上层使用。

(6) 流量控制和缓存。传输层也有流量控制功能。传输层的流量控制主要是通过可变滑动窗口协议来实现的。所谓可变滑动窗口协议，是指发送方的发送窗口大小是由接收方根据自己的实际接收情况向发送方报告确定的，所以是可变的。

(7) 差错控制。对于传输层的数据单元，传输过程中数据有可能会丢失、重复、顺序颠倒或出现错误等，因此，传输层必须有错误检测和恢复的能力。

2.2.6 会话层

所谓会话，既可以是两个实体之间建立数据交换的连接，也可以是这两个实体之间通信和交换的所有状态的记录。会话层(session layer)负责在网络中的两个节点之间建立和维持通信、建立会话和拆除会话等会话管理服务。

会话层的主要功能包括：建立通信连接，保持会话过程通信连接的畅通，使两个会话实体之间的会话保持同步，决定通信是否被中断及通信中断时决定从何处重新发送。

会话层的主要特点如下：

(1) 将会话地址映射为传输地址。

(2) 选择需要的传输服务质量(QoS)参数。

(3) 对会话参数进行协商。

(4) 识别各个会话连接。

（5）数据传输。
（6）连接释放。

2.2.7 表示层

表示层(presentation layer)位于会话层之上,负责处理通信实体间会话的语法,它从应用层获得数据并按照协议语法进行格式转换,经格式转换的信息可供网络通信使用。也就是说,表示层在用户的应用进程与网络之间进行数据格式的转换,使得差别很大的系统中的进程之间可以相互通信,因为表示层可以先将数据转换成网络所能理解的格式以进行传输,然后再转换成目标系统进程所能够理解的数据格式。

表示层还负责对数据进行加密与解密。在发送重要数据时,表示层对其进行加密;在接收数据时则负责进行解密。此外,表示层协议还会对图片和文件格式信息进行解码和编码。

2.2.8 应用层

应用层(application layer)是 OSI 参考模型的最高层,处理实体间通信的语义详解,应用进程通过应用层协议实现为用户提供最终服务。尽管它被称为应用层,但它并不包含任何用户应用,相反,它只在应用进程和网络服务之间提供接口。

应用层包含许多协议,这些应用层协议对于需要通信的应用进程来说都是必需的。例如,当远程终端通过远程登录服务登录到主机时,远程登录的应用进程需要获得应用层协议的支持和服务,才能将数据传给会话层。由于当前网络所能够提供的应用和服务的类型越来越丰富和多样化,所以应用层必须面对各种要求不同的应用进程,并且存在非常多的不同应用层实体。应用层是 OSI 参考模型中最丰富的一个层次。随着应用的不断发展,应用层的内容还会不断丰富,不同的应用实体很可能会面对同一个实体协议。

2.3 TCP/IP 因特网应用模型

TCP/IP 是一组通信协议的总称,它是因特网(Internet)的核心,利用 TCP/IP 协议可以很方便地实现多个网络的无缝连接,就是指该主机具有一个因特网地址(也称 IP 地址),运行 TCP/IP 协议,并可向因特网上所有其他主机发送 IP 数据报。

TCP/IP 具有如下特点:

（1）开放的协议标准,可以免费使用,并且独立于特定的计算机硬件与操作系统。
（2）独立于特定的网络硬件,可以运行在局域网和广域网,更适用于因特网中。
（3）统一的网络地址分配方案,使得整个 TCP/IP 设备在网络中都具有唯一的地址。
（4）标准化的高层协议,可以提供多种可靠的用户服务。

2.3.1 TCP/IP 的层次结构

TCP/IP 分为 4 个层次，分别是网络接口层、网际层、传输层和应用层。TCP/IP 的层次结构与 OSI 层次结构的对照关系如图 2-4 所示。

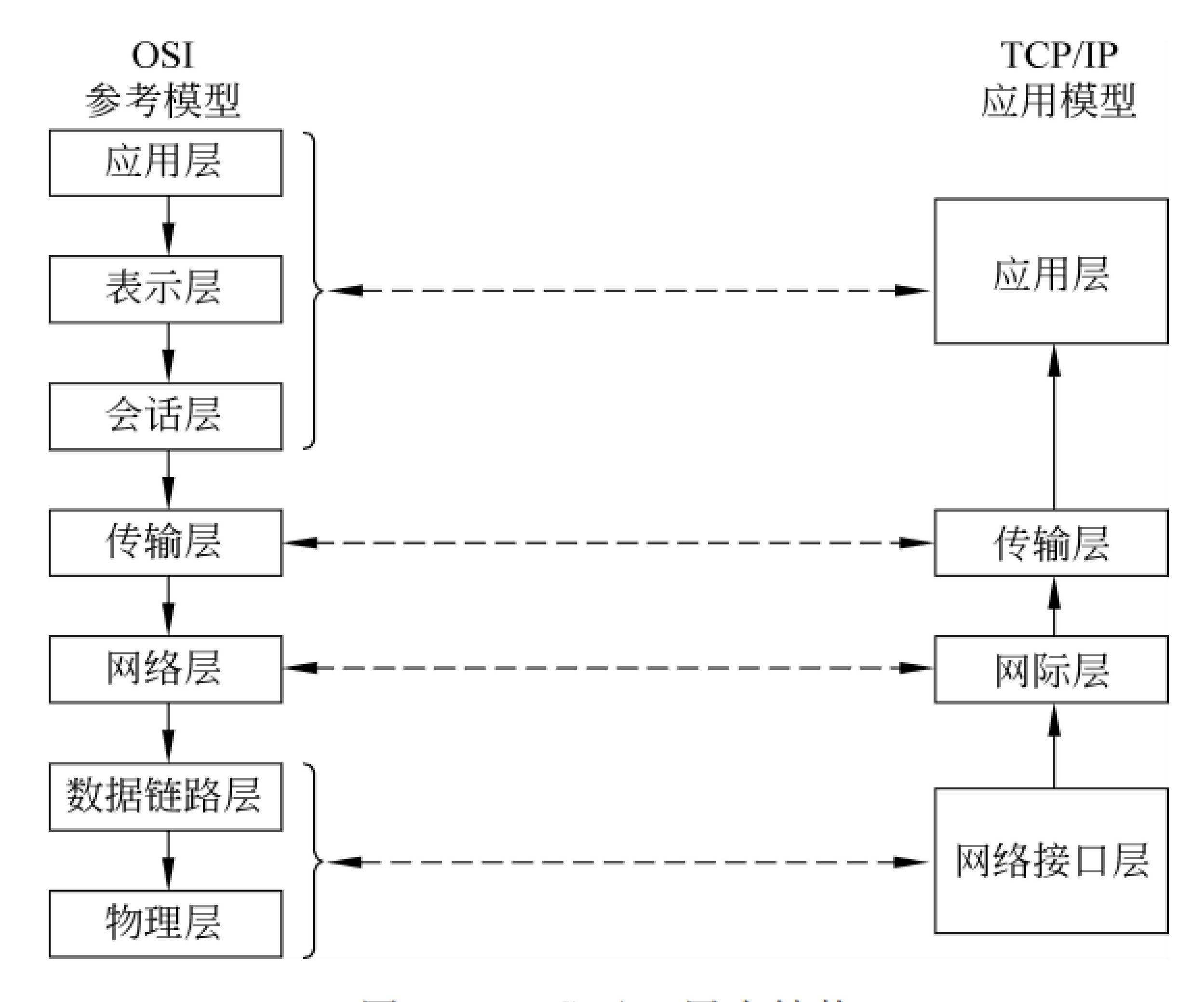


图 2-4 TCP/IP 层次结构

1. 网络接口层

网络接口层是 TCP/IP 协议的最底层，负责接收 IP 数据包并通过网络发送 IP 数据包；或者从网络上接收数据帧，取出 IP 数据包，并把它交给网络层。网络接口一般是设备驱动程序，如以太网的网卡驱动程序。

2. 网际层

网际层(或称网络互联层)所执行的主要功能是处理来自传输层的分组，将分组形成数据包，并为该数据包进行路径选择，最终将数据包从源主机发送到目的主机。在网际层中，最常用的协议是网际协议 IP，其他一些协议用来协助 IP 的操作。

3. 传输层

传输层提供应用程序间的通信，提供了差别传输。其中 TCP 提供可靠传输，UDP 提供不可靠的传输。为了实现传输可靠性，传输层要进行必要的数据报收发确认，若数据丢失则进行重传，强化了信息校验功能。

4. 应用层

在 TCP/IP 模型中，应用程序接口是最高层，它与 OSI 参考模型中的高三层的任务相

同,用于提供网络服务,比如文件传输(FTP)、远程登录(Telnet)、域名服务(DNS)、简单邮件传输(SMTP)、简单网络管理(SNMP)以及超文本传输(HTTP)等。

2.3.2 TCP/IP 协议

TCP/IP 协议其实是一组(族)协议,它包括许多协议,组成了 TCP/IP 协议族,见图 2-5。但传输控制协议(TCP)和网际协议(IP)是其中最重要的确保数据完整传输的两个协议。

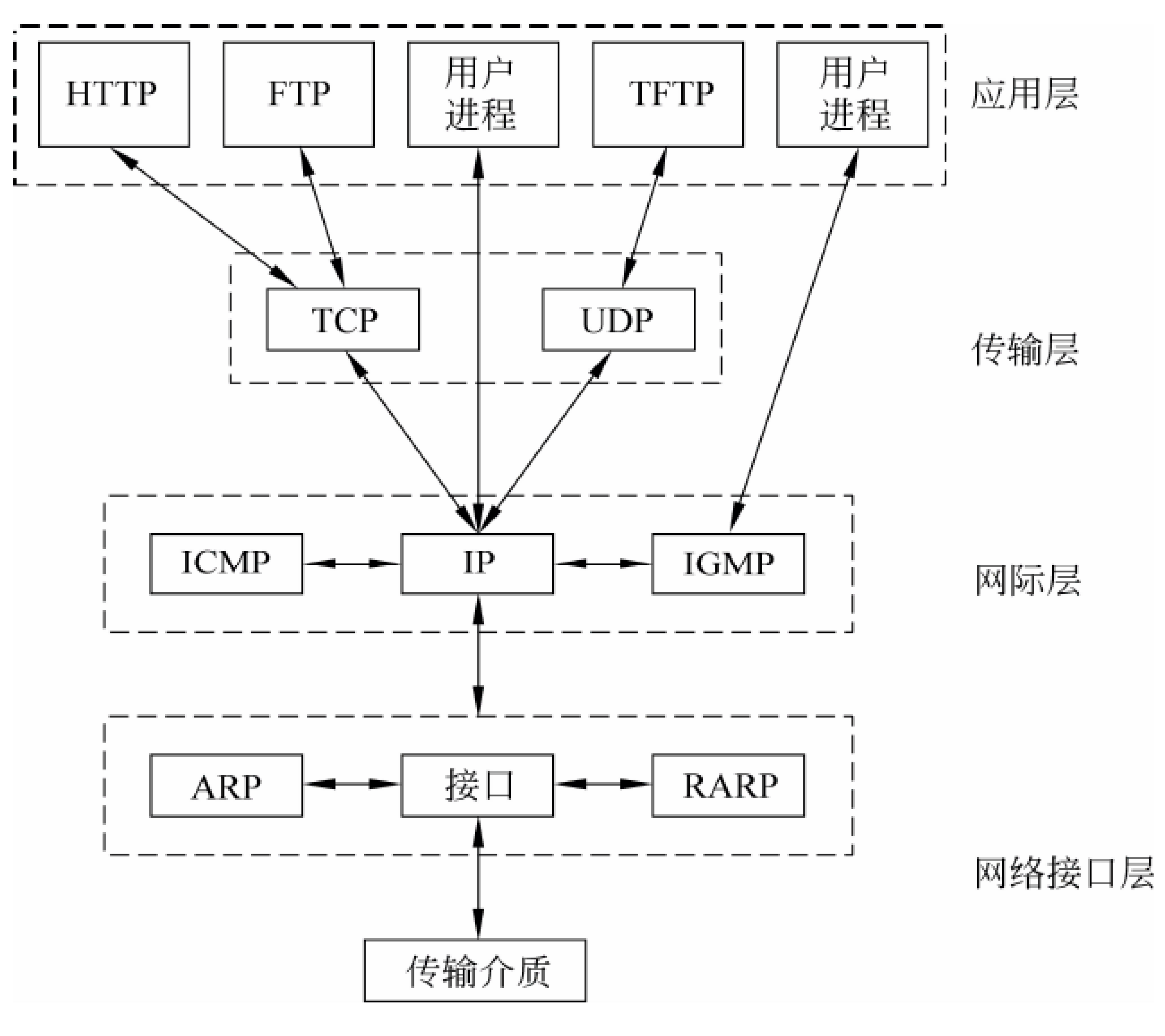


图 2-5 TCP/IP 层次协议

TCP/IP 协议的基本传输单位是数据包,TCP/IP 协议负责把数据分成若干数据包,并给每个数据包加上包头,每个的包头再加上接收端的地址。如果传输过程中出现数据丢失、数据失真等情况,TCP/IP 协议会自动要求数据重新传输,并重新组包。

IP 协议保证数据的传输,TCP 协议确保数据传输的质量。

1. TCP/IP 的网络接口层

(1) SLIP 协议。SLIP 提供在串行通信线路上封装 IP 分组的简单方法,用以使远程用户通过电话线和 Modem 能方便地接入 TCP/IP 网络。

SLIP 提供简单的组帧方式,在实际应用中存在一些问题。首先,SLIP 不支持在连接过程中的动态 IP 地址分配,通信双方必须事先告知对方 IP 地址,这给没有固定 IP 地址的个人用户上因特网带来了很大的不便。其次,SLIP 帧中无协议类型字段,因此它只能支持 IP 协议。

(2) PPP 协议。为了解决 SLIP 存在的问题,在串行通信应用中又开发了 PPP 协议。PPP 协议是一种有效的点对点通信协议,它是串行通信线路上的组帧方式,用于建立、配

制、测试和拆除数据链路，包括链路控制协议，(Link Control Protocol，LCP)、网络控制协议(Network Control Protocol，NCP)、常用口令认证协议(Password Authentication Protocol，PAP)和握手验证协议(Challenge-Handshake Authentication Protocol，CHAP)等。

由于 PPP 帧中设置了校验字段，因而 PPP 在链路层上具有差错检验的功能。PPP 中的 LCP 协议提供了通信双方进行参数协商的手段，并且提供了一组 NCP 协议，使得 PPP 可以支持多种网络层协议，如 IP、IPX、OSI 等。另外，支持 IP 的 NCP 提供了在建立连接时动态分配 IP 地址的功能，解决了个人用户接入因特网的问题。

2. TCP/IP 网际层

网际层中含有 4 个重要的协议：网际协议(IP)、互联网控制报文协议(ICMP)、地址转换协议(ARP)和反向地址转换协议(RARP)，网际层的功能主要由 IP 来提供。除了提供端到端的分组分发功能外，IP 还提供了很多扩充功能。例如，为了克服数据链路层对帧大小的限制，网际层提供了数据分组和重组功能，这使得很大的 IP 数据报能以较小的分组在网上传输。

(1) 网际协议。网际层最重要的协议是网际协议(Internet Protocol，IP)，它将多个网络连成一个互联网，可以把高层的数据以多个数据报的形式通过互联网分发出去。

IP 的基本任务是通过互联网传送数据报，各个 IP 数据报之间是相互独立的。主机上的网际层向传输层提供服务。IP 从源传输实体取得数据，通过它的网络接口层服务传给目的主机的网际层。IP 不保证服务的可靠性，在主机资源不足的情况下，它可能丢弃某些数据报，同时 IP 也不检查被数据链路层丢弃的报文。在传送时，高层协议将数据传送到网际层，网际层再将数据封装为互联网数据报，并交给数据链路层协议通过局域网传送。若目的主机直接连在本网中，IP 可直接通过网络将数据报传给目的主机；若目的主机在远程网络中，则 IP 对数据报进行路由选择，并把它投递到路由器中，路由器则依次通过下一网络将数据报传送到目的主机或再下一个路由器，即一个 IP 数据报是通过互联网从一个 IP 模块传到另一个 IP 模块，直到终点为止。

(2) 互联网控制报文协议(ICMP)。从互联网协议的功能，可以知道 IP 提供的是一种不可靠的分组传送服务。若路由器故障使网络阻塞，就需要通知发送主机采取相应措施。为了使互联网能报告差错，或提供有关意外情况的信息，在 IP 层加入了一类特殊用途的报文机制，即互联网控制报文协议(ICMP)。

(3) 地址转换协议(ARP)。在 TCP/IP 网络环境下，每个主机都分配了一个 32 位的 IP 地址，这种互联网地址是在国际范围内标识主机的一种逻辑地址。为了让报文在物理网上传送，必须知道彼此的物理地址。这样就存在把互联网地址变换为物理地址的地址转换问题。以以太网(Ethernet)环境为例，为了正确地向目的站传送报文，必须把目的站的 32 位 IP 地址转换成 48 位以太网目的物理地址(MAC)。这就需要在网际层有一组服务将 IP 地址转换为相应的物理网络地址，这组协议即 ARP。

在进行报文发送时，如果源网际层给的报文只有 IP 地址，而没有对应的以太网地址，则网际层广播 ARP 请求以获取目的站信息，而目的站必须回答该 ARP 请求。这样源站

点可以收到以太网48位物理地址，并将地址放入相应的高速缓存(Cache)。下一次源站点对同一目的站点的地址转换可直接引用高速缓存中的地址内容。地址转换协议(ARP)使主机可以找出同一物理网络中任一物理主机的物理地址，只需给出目的主机的IP地址即可。这样，网络的物理编址可以对网络层服务透明。

(4) 反向地址转换协议(RARP)。该协议用于一种特殊情况。如果站点初始化以后，只有自己的物理地址而没有IP地址，则它可以通过RARP协议发出广播请求，征求自己的IP地址，而RARP服务器则负责回答。这样，无IP地址的站点可以通过RARP协议取得自己的IP地址，这个地址在下一次系统重新开始以前都有效，不用连续广播请求。

3. TCP/IP传输层

TCP/IP在这一层提供了两个主要的协议：传输控制协议(TCP)和用户数据报协议(UDP)。

(1) 传输控制协议(TCP)。该协议提供的是一种可靠的数据流服务。当传送因受差错干扰，或基础网络故障，或网络负荷太重而使传输系统不能正常工作时，就需要通过其他协议来保证通信的可靠。TCP就是这样的协议，它对应于OSI参考模型的传输层，它在IP协议的基础上提供端到端的面向连接的可靠传输。

TCP采用自动检测传输被损坏或被丢失的数据报，自动重传来实现传输的可靠性。通信的接收方每接收一次数据就送回一个确认报文，发送方对每个发出去的报文都留一份记录，等到收到确认之后再发出下一报文分组。发送方发出一个报文分组时，启动一个计时器，若计时器计数完毕，确认报文还未到达，则发送方重新发送该报文分组。

简单地确认重传严重浪费带宽，因此TCP还采用一种称之为“滑动窗口”的流量控制机制来提高网络的吞吐量，窗口的范围决定了发送方发送的但未被接收方确认的数据报的数量。每当接收方正确收到一则报文时，窗口便向前滑动，这种机制使网络中未被确认的数据报数量增加，提高了网络的吞吐量。

TCP通信建立在面向连接的基础上，实现了一种“虚电路”的概念。双方通信之前，先建立一条连接，然后双方就可以在其上发送数据流。这种数据交换方式能提高效率，但事先建立连接和事后拆除连接需要开销。TCP连接的建立采用三次握手的过程，整个过程由发送方请求连接、接收方发送确认信息和发送方再发送确认信息3个过程组成，见图2-6。

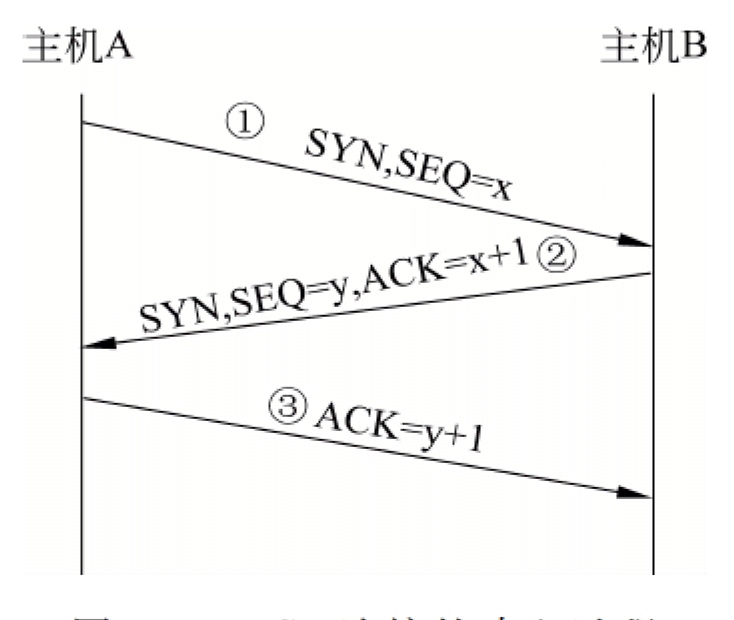


图2-6　TCP连接的建立过程

(2) 用户数据报协议(UDP)。该协议是对IP协议族的扩充，它增加了一种机制，发送方使用这种机制可以区分一台计算机上的多个接收者。每个UDP报文除了包含某用户进程发送的数据外，还有报文目的端口的编号和报文源端口的编号。UDP的这种扩充使得在两个用户进程之间递送数据报成为可能。

UDP是依靠IP协议来传送报文的，因而它的服务和IP一样是不可靠的。这种服务不用确认、不对报文排序，也不进行流量控制，UDP报文可能会出现丢失、重复和失序等现象。

4. TCP/IP的应用层

TCP/IP的上3层与OSI参考模型有较大区别，也没有非常明确的层次划分。其中SMTP、FTP、HTTP、DNS和Telnet是几个在各种不同的机型上广泛实现的协议，TCP/IP中还定义了许多别的高层协议。

(1) 文件传输协议(FTP)。文件传输协议是网际提供的用于访问远程机器的一个协议，它使用户可以在本地机与远程机之间进行有关文件的操作。FTP工作时建立两条TCP连接，一条用于传送文件，另一条用于传送控制。

FTP采用客户/服务器模式，它包含客户FTP和服务器FTP。客户FTP启动传送过程，而服务器对其做出应答。客户FTP大多有一个交互式界面，使客户可以灵活地向远地传文件或从远地取文件。

(2) 远程终端访问协议(Telnet)。远程终端访问协议的连接是一个TCP连接，用于传送具有Telnet控制信息的数据。它提供了与终端设备或终端进程交互的标准方法，支持终端到终端的连接及进程到进程分布式计算的通信。

(3) 域名服务协议(DNS)。域名服务协议是一个域名服务的协议，提供域名到IP地址的转换，允许对域名资源进行分散管理。DNS最初设计的目的是使邮件发送方知道邮件收发双方主机的IP地址，后来发展成为可服务于许多其他目标的协议。

(4) 简单邮件传送协议(SMTP)。互联网标准中的电子邮件是一个单向的基于文件的协议，用于可靠、有效的数据传输。SMTP作为应用层的服务，并不关心它下面采用的是何种传输服务，它可能通过网络在TCP连接上传送邮件，或者简单地在同一计算机的进程之间，通过进程通信的通道来传送邮件。这样，邮件传输就独立于传输子系统，可在TCP/IP环境、OSI传输层或X.25协议环境中传输邮件。邮件发送之前必须协商好发送者和接收者。SMTP服务进程同意为接收方发送邮件时，它将邮件直接交给接收方用户，或者将邮件经过网络连接器交给接收方用户。在邮件传输过程中，所经过的路由被记录下来，这样，当邮件不能正常传输时可按原路由找到发送者。

2.3.3 两种分层结构的比较

将OSI参考模型与TCP/IP模型比较，可以看出以下特点：

(1) 两者都是层次结构的模型。

(2) 两者的最底层都是面向通信子网。

(3) 两个模型都有传输层，且都是第一个提供端到端数据传输服务的层次，都能提供面向连接或无连接传输服务。

(4) 两者的最高层都是向各种用户应用进程提供服务的应用层。

(5) 两者所划分的层次数不同。

(6) TCP/IP 中没有表示层和会话层。

(7) TCP/IP 没有明确规定通信子网的协议,也不再区分通信子网中的物理层、数据链路层和网络层。

(8) TCP/IP 中特别强调了网际层,其中运行的 IP 协议是因特网的核心协议,且网际层向上只提供无连接的服务,而不提供面向连接的服务等。

OIS 参考模型是由 ISO 和 ITU-T(原 CCITT)共同制定的国际标准,它提供了一个比较系统完整地反映计算机网络体系结构的参考模型。它吸收了当时已有的由各个公司自己规定的网络体系结构的基本思想与优点,但又不等同于其中任何一个。后来,ISO 和原 CCITT 又在这个参考模型的框架内为各个层次制定了一系列的协议标准和服务规范,构成了庞大的 OSI 基本标准集。

20 世纪 80 年代末和 90 年代初,许多专家都认为 OSI 参考模型及其协议将取代所有其他模型及协议,但是这并没有成为事实。虽然现在 OSI 参考模型仍为国际上普遍认同,并且许多网络在描述和说明时仍以这个参考模型作为标准来对照,OSI 标准集中的某些协议也已得到实现和广泛的应用,但是至今并没有一个实际运行的网络是完全按照 OSI 参考模型和协议来构建的。这既有技术上的原因,比如说这个模型和协议过于庞大复杂,如何对其进行裁剪及在实现后如何对符合标准的程度进行一致性测试等问题尚未完全解决,也有不适当的策略和时机等因素。OSI 参考模型和协议虽然得到了各国政府部门和官方的明确支持,但是仅靠官方来推动的策略并不一定能决定技术的发展方向。

20 世纪 90 年代以后,因特网迅速发展,已经形成了一股难以阻挡的潮流。TCP/IP 和 OSI 参考模型完全不一样,不是先给出参考模型而后再规定每层的协议,而是先有协议,网络实际运行后再总结出参考模型。TCP/IP 中的核心协议 TCP 和 IP 是被仔细设计的,并且很好地实现了。在 TCP/IP 参考模型中并没有明显地区分服务和协议,它不是通用的,不适宜于用来描述其他的网络系统,甚至没有区分数据链路层和物理层。严格说来,TCP/IP 模型不是一个官方的国际标准,但是由于 TCP/IP 影响巨大,已成为一种事实上的国际工业标准。

2.4 IP 地址和子网掩码

在因特网中,为了使众多的主机能够相互识别,通常要给每一台主机分配一个唯一的 IP 地址,也称网际地址。

2.4.1 IP 地址

1. IP 地址的组成

目前的 IP 地址是一个 32 位的二进制数,由地址类别、网络标识和主机标识 3 部分组成,如图 2-7 所示。

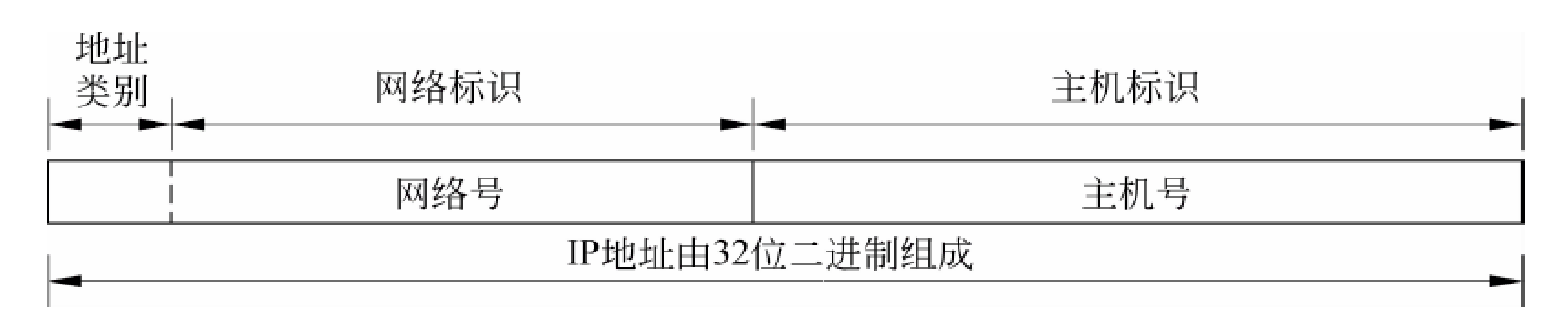


图 2-7 IP 地址组成

2. IP 地址的分类

IP 地址分成 A 类、B 类、C 类、D 类和 E 类，这 5 类地址划分方法见图 2-8。

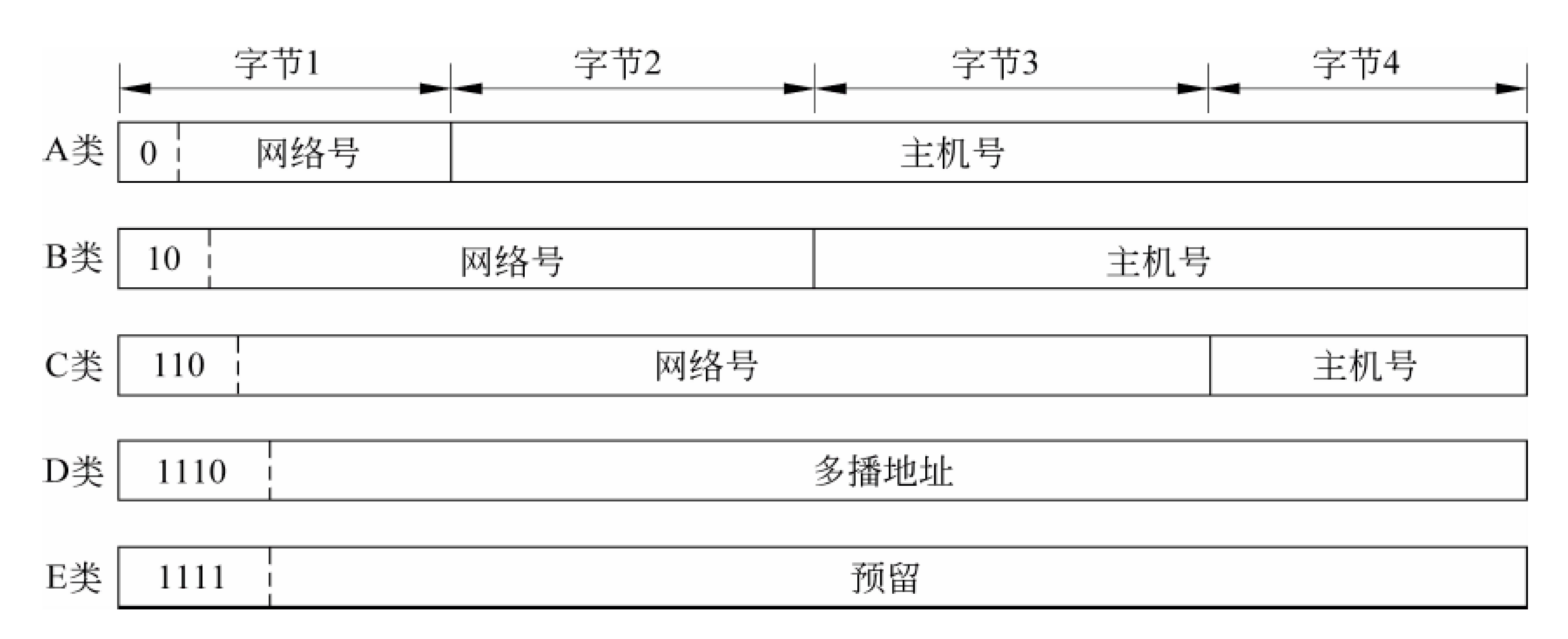


图 2-8 5 类 IP 地址划分

1）A 类地址

A 类地址网络号占 1 个字节，主机号占 3 个字节，并且规定第一个字节的最高位为 0，用来表示地址是 A 类地址，二进制数值范围为 00000000～01111111。理论上，A 类地址的网络数为 2^7(128)，每个网络包含的主机数为 2^{24}(16 777 216)，A 类地址(点分十进制)的范围是 0.0.0.0～127.255.255.255。

特殊规定：A 类地址中，网络号全为 0 和全为 1 保留用于回路与诊断测试，主机号全为 0 和全为 1 用作网络标识与广播地址。

因此实际应用中，A 类地址有效的网络数为 128－2＝126 个，其范围是 1～126。每个 A 类网络实际的主机数应该是 $2^{24}-2$＝16 777 214 台。所以，A 类网主机可以使用的地址有效范围是 1.0.0.1～126.255.255.254。

2）B 类地址

B 类地址网络号和主机号各占两个字节，并且第一个字节的最高两位为 10，用来表示地址是 B 类地址，二进制数值范围为 10000000 ～10111111。因此 B 类地址有效网络数为 2^{14}(16 384)。特殊规定：B 类网络地址类中主机号全 0 和全 1 用作网络标识与广播。所以，每个 B 类网络号所包含的主机数为 $2^{16}-2$＝65 534 台。B 类网络主机地址有效范围为 128.0.0.1～191.255.255.254。

3）C 类地址

C 类地址网络号占 3 个字节，主机号占 1 个字节，并且第一个字节的最高 3 位为 110，

用来表示地址是 C 类地址，二进制数值范围为 11000000～11011111。因此 C 类地址有效网络数为 2^{21}(2 097 152)个。特殊规定：C 类网络地址类中主机号全 0 和全 1 用作网络标识与广播。所以，每个网络号所包含的主机数为 $2^8-2=254$ 台。C 类网络主机地址有效范围为 192.0.0.1～223.255.255.254。

4）D 类地址

D 类地址用于组播组用户，组播就是同时把数据发送给一组主机，只有那些已经登记可以接收组播地址的主机才能接收组播。D 类地址的范围是 224.0.0.0～239.255.255.255。

5）E 类地址

E 类地址是为将来预留的，同时也可以用于实验目的，它们不能被分配给主机。E 类地址第一字节的数值范围是 240～255。

其中，A、B、C 类地址是基本的因特网地址，是用户使用的地址，为主类地址。D、E 类地址为次类地址，有特殊用途，为系统保留。表 2-5 列出了 IP 地址的使用范围。

表 2-5 IP 地址的使用范围

网络类型	第一个字节范围	可用网络号范围	最大网络数	每个网络中的最大主机数
A	0～127	1～126	126(2^7-2)	16 777 214($2^{24}-2$)
B	128～191	128.0～191.255	16 384(2^{14})	65 534($2^{16}-2$)
C	192～233	192.0.0～223.255.255	2 097 152(2^{21})	254(2^8-2)

2.4.2 子网掩码与子网的划分

子网掩码是与 IP 地址配合使用的技术，主要用来解决两个问题，一是快速区分 IP 地址中的网络标识与主机标识，二是解决大型 IP 网络划分子网问题。

1. 子网掩码

子网掩码(subnet mask)与 IP 地址相同，也是一个“点分十进制”表示的 32 位二进制数，通过子网掩码，可以指出一个 IP 地址中的哪些位对应于网络地址(网络号)，哪些位对应于主机地址(主机号)。对于子网掩码的取值，通常是将对应于 IP 地址中网络地址的所有位都设置为 1，对应于主机地址的所有位都设置为 0。

默认情况下，A、B、C 三类网络的子网掩码如表 2-6 所示。

表 2-6 A、B、C 三类网络默认的子网掩码

地址类型	点分十进制数	子网掩码的二进制位			
A	255.0.0.0	11111111	00000000	00000000	00000000
B	255.255.0.0	11111111	11111111	00000000	00000000
C	255.255.255.0	11111111	11111111	11111111	00000000

子网掩码的作用是判断信源主机和信宿主机是否在同一网段上，方法是把信源主机

地址和信宿主机地址分别与所在网段的子网掩码进行二进制"与"运算，如果产生的两个结果相同，则在同一网段；如果产生的结果不同，则两台主机不在同一网段，这两台计算机要进行相互访问时，必须通过一台路由器进行路由转换。

例如，某A主机的IP地址为210.110.200.62，子网掩码为255.255.255.0，计算其网络号。

210.110.200.62 →11010010 01101110 11001000 00111110

255.255.255.0 →11111111 11111111 11111111 00000000

与运算后的结果：→11010010 01101110 11001000 00000000

转换为十进制： 210 110 200 0

因此，IP地址210.110.200.62的网络地址是210.110.200。

2. 子网划分

在实际应用中，常常将一个较大的网络分成几个部分，每一个部分称为一个子网(或网段)，见图2-9。

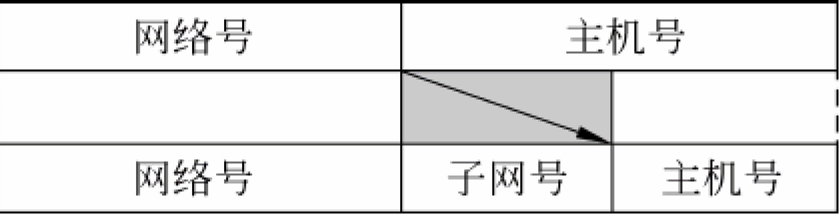


图2-9 子网的划分

其中，表示子网号的二进制位数(借用主机地址位数)取决于子网的个数，假设占用主机地址的位数为m，子网个数为n，它们之间的关系是$2^m=n$。

例如，一个B类网络163.101.0.0将主机号分为两部分，其中8位二进制用于子网号，另外8位二进制用于主机号，那么这个B类网络就可被分为254个子网，每个子网可以容纳254台主机。

下面以C类子网为例，说明各种掩码所能划分的子网数目，如表2-7所示。

表2-7 子网掩码与主机数

子网数目	占用位数	子网掩码	子网中主机数
0	0	255.255.255.0	254
2	1	255.255.255.128	126
4	2	255.255.255.192	62
8	3	255.255.255.224	30
16	4	255.255.255.240	14
32	5	255.255.255.248	6
64	6	255.255.255.252	2

2.4.3 几种特殊的IP地址

在因特网中，有些IP地址具有特定用途。

(1) 网络地址。由一个有效的网络号和一个全0的主机号组成，用来表示某一个具

体的网络。例如地址128.0.0.0表示128.0的B类网络。

(2) 广播地址。由一个有效的网络号和一个全1的主机号构成,其作用是因特网的主机向网络号所指向的网络广播信息。例如,202.103.225.255是网络号为202.103.225.0的网络的广播地址。

特殊情况是:32位全为1的IP地址(255.255.255.255)用于本网广播。

(3) 回环地址。A类网络的网络号为127(即01111111)的IP地址是保留地址,可作为本地软件回环测试主机,叫做回环地址。即在127.0.0.0～127.255.255.255之间,除了主机号为全0(127.0.0.0)或主机号为全1(127.255.255.255)以外都是可用的回环地址。因此,含有网络号127的数据报不可能出现在任何网络上。

(4) 专用地址。由于IP地址的紧缺,一个机构能够申请到的IP地址数目往往远小于本机构所拥有的主机数。而且,出于安全等原因,一个机构内的很多主机并不需要接入到外部的因特网,它们主要是和内部的其他主机进行通信。因此,对于这些机构内部的主机来说,只需使用仅在本机构有效的本地IP地址即可,不需要向因特网的管理机构申请全球唯一的IP地址。

为了解决机构内部主机使用IP地址的问题,因特网的管理机构定义了一些专用地址,也称为本地地址或私有地址。这些IP地址只能用于机构的内部通信,不能和因特网上的其他主机通信。也就是说,因特网中的所有路由器不转发使用专用地址的主机的数据报。

专用地址如下:

(1) 10.0.0.0～10.255.255.255(一个A类网络)。

(2) 172.16.0.0～172.31.255.255(16个连续的B类网络)。

(3) 192.168.0.0～192.168.255.255(256个连续的C类网络)。

2.5 本章小结

计算机网络是由某地域(或全球)范围内的多台计算机系统通过通信系统连接而成的一个复杂系统,如何构造计算机系统的通信功能才能实现这些计算机系统之间,尤其是异构计算机系统之间的相互通信,这是网络体系结构着重要解决的问题。本章详细介绍了两种网络体系结构模型:OSI参考模型和TCP/IP互联网应用模型。TCP/IP模型目前是业界的实际应用标准,并在此基础上介绍了IP地址划分及子网掩码应用。

综合训练

一、理论题

1. 选择题

(1) 计算机网络体系结构是用(　　)方法去分析计算机网络这个复杂事物,以达到

从抽象角度去把握和理解计算机网络概念的目的。

A. 复杂化　　B. 结构化、层次化　　C. 程序化　　D. 国际标准化

(2) 层次结构提供了一种按层次来观察网络的方法,它描述了网络中任意(　　)间的逻辑连接和信息传输。

A. 计算机设备　　B. 通信设备　　C. 两个节点　　D. 两个用户

(3) 在下列功能中,最好地描述了 OSI 参考模型的数据链路层的是(　　)。

A. 保证数据正确的顺序、无错和完整　　B. 处理信号通过介质的传输

C. 提供用户与网络的接口　　D. 控制报文通过网络的路由选择

(4) OSI 参考模型的物理层负责的功能是(　　)。

A. 格式化报文　　B. 数据选择通过网络的路由

C. 定义连接到介质的特征　　D. 提供远程文件访问能力

(5) 在不同网络节点的对等层之间的通信需要(　　)。

A. 模块接口　　B. 对等层协议　　C. 电信号　　D. 传输介质

(6) 在 TCP/IP 参考模型中,与 OSI 参考模型的网络层对应的是(　　)。

A. 应用层　　B. 网际层　　C. 表示层　　D. 传输层

(7) 在 TCP/IP 中,UDP 协议是一种(　　)协议。

A. 传输层　　B. 网络网际层　　C. 表示层　　D. 应用层

2. 填空题

(1) OSI 参考模型的全称是________,从底层到高层分别是________。

(2) 传输层是计算机网络中的________和________的接口和桥梁。

(3) 数据链路层完成差错控制、链路管理和________控制。

(4) TCP/IP 模型共分为________、________、________和________ 4 个层次。

(5) 网络接口层是 TCP/IP 协议的________。

3. 简答题

(1) 网络协议的三要素是什么?

(2) 数据报与虚电路操作各有什么特点?

(3) 数据报服务与虚电路服务各有什么特点?

(4) TCP/IP 协议模型分为几层? 各层的功能是什么? 每层又包含什么协议?

(5) 试述数据链路层的主要功能,并说明物理链路与数据链路的区别。

(6) 简述 OSI 参考模型与 TCP/IP 模型的异同点。

二、实践题

1. TCP/IP 子网划分与测试

参考步骤如下:

(1) 安装有 Windows XP/2003 系统的计算机对等网。

(2) 将班级划分成 6～8 个实验小组，每个实验小组指定一个独立的 C 类网络地址，验证同一小组以及不同小组的网络中主机的连通性。

例如，各小组的网络号和主机号如下：

小组编号 网络号 主机号

1 组：192.168.1　1～254

2 组：192.168.2　1～254

3 组：192.168.3　1～254

4 组：192.168.4　1～254

5 组：192.168.5　1～254

6 组：192.168.6　1～254

7 组：192.168.7　1～254

8 组：192.168.8　1～254

(3) 班级组建一个 C 类网络，每个小组建一个子网，每个小组 6～8 个人，计划组建 8 个子网。设置一个 C 类网络(例如 192.168.1)，请分别写出 8 个子网地址(见表 2-8)。

表 2-8　子网划分地址一览表

子网划分 第 4 字节前 3 位	子网地址范围	子网广播地址	子网有效地址范围
000	192.168.1.0～31/27	192.168.1.31/27	192.168.1.1～30/27
001	192.168.1.32～63/27	192.168.1.63/27	192.168.1.33～62/27
010	192.168.1.64～95/27	192.168.1.95/27	192.168.1.65～94/27
011	192.168.1.96～127/27	192.168.1.127/27	192.168.1.97～126/27
100	192.168.1.128～159/27	192.168.1.159/27	192.168.1.129～158/27
101	192.168.1.160～191/27	192.168.1.191/27	192.168.1.161～190/27
110	192.168.1.192～223/27	192.168.1.223/27	192.168.1.193～222/27
111	192.168.1.224～255/27	192.168.1.255/27	192.168.1.225～254/27

2. 配置 TCP/IP 协议参数

通过 Windows 操作系统，认识和理解 TCP/IP 协议，正确配置 TCP/IP 协议参数。

参考步骤如下：

(1) 选择“开始”→“运行”，在“运行”窗口输入 cmd，见图 2-10。

(2) 在命令提示符窗口中输入 ipconfig，测试本地连接地址信息，见图 2-11。

(3) 在桌面右击“网上邻居”，在快捷菜单中选择“属性”，在打开的“网络连接”对话框中右击

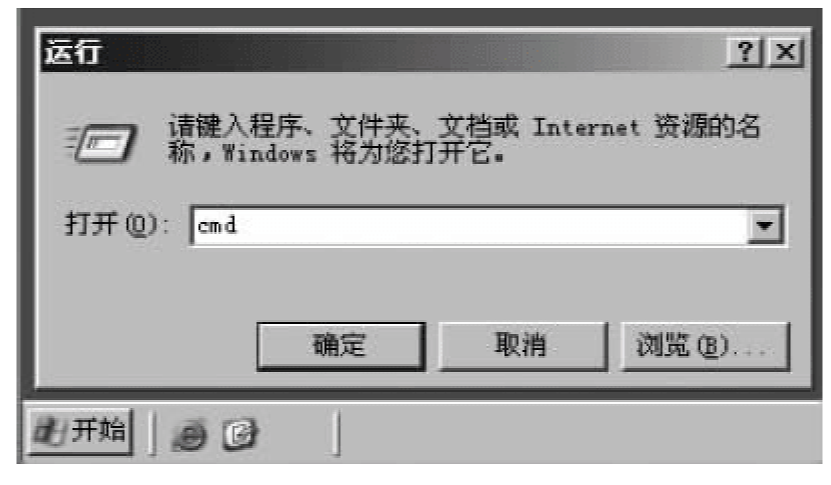


图 2-10　“运行”窗口

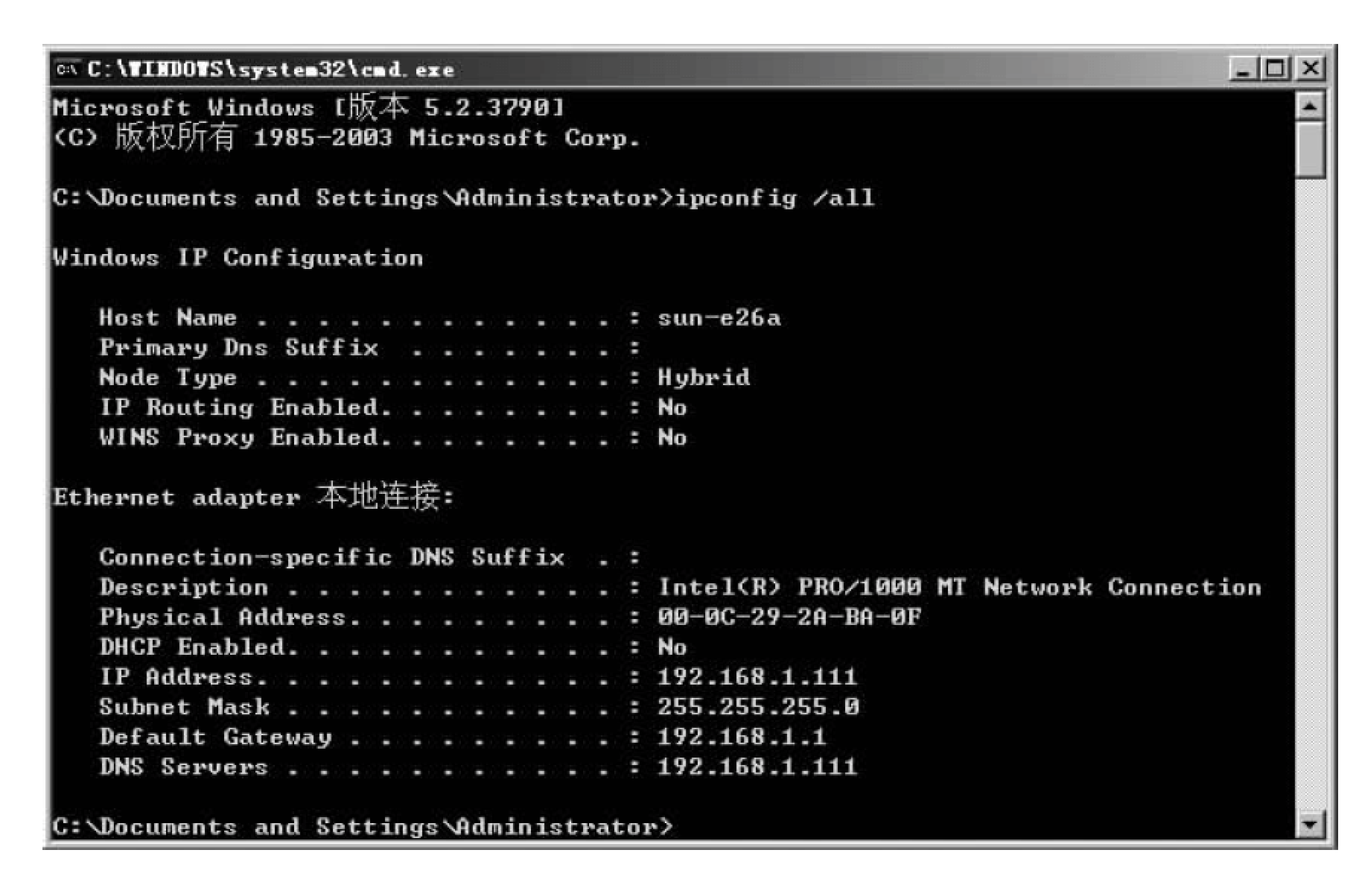


图 2-11 本地连接信息

“本地连接”,在快捷菜单中选择“属性”,双击“此连接使用下列项目”列表中的 Internet 协议(TCP/IP)选项,打开“Internet 协议(TCP/IP)属性”对话框,见图 2-12。



图 2-12 TCP/IP 属性设置

(4) 在该对话框中,选择“使用下面的 IP 地址”单选按钮,将第(2)步记录的地址信息填入相应的位置,见图 2-12。

(5) 在该话框中单击“高级”按钮，了解 TCP 端口和 UDP 端口，添加如下常用端口：HTTP 为 80 端口，FTP 为 21 端口，进行实验测试，见图 2-13。

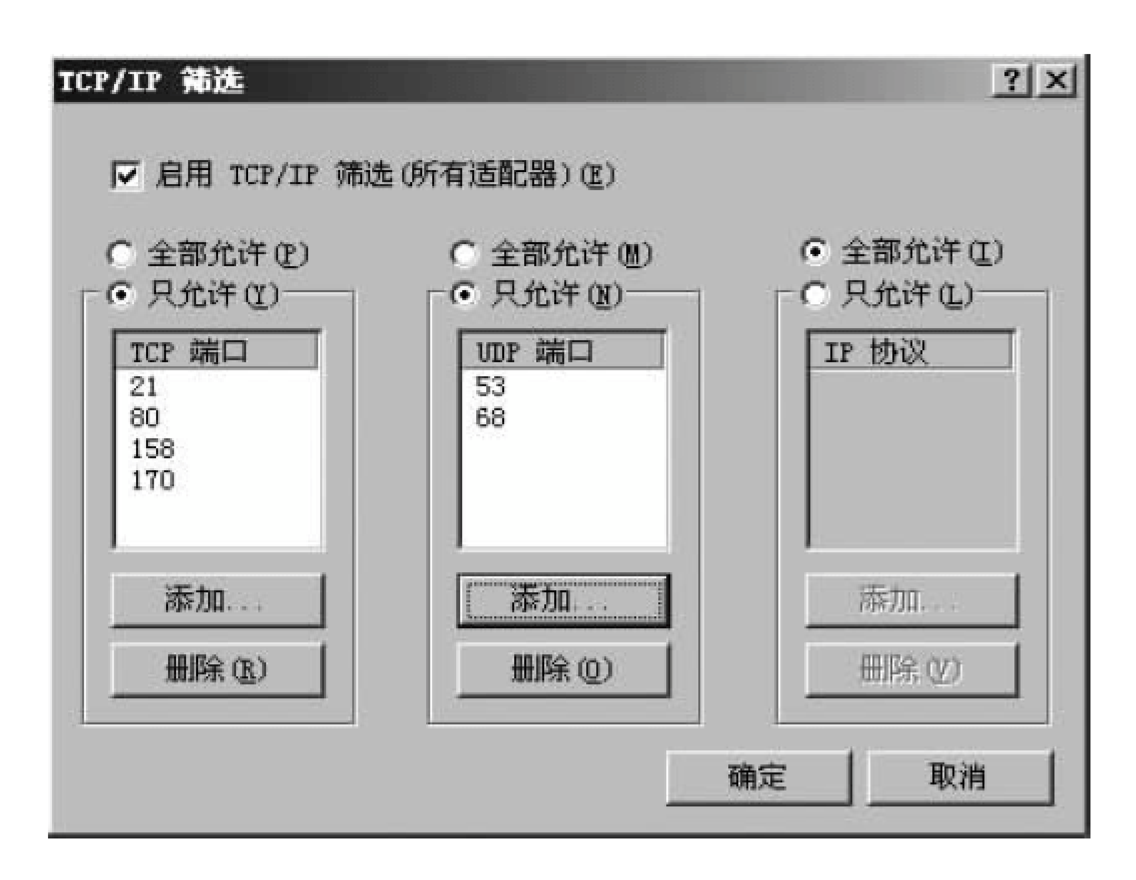


图 2-13　TCP/IP 端口筛选

第3章　计算机局域网技术

本章主要内容

- 局域网的特点、功能及其分类
- 局域网体系结构
- 传输介质访问控制方式
- IEEE 802与以太网
- 虚拟局域网
- 无线局域网

计算机局域网技术适用在局部地域范围内组网，实现局域内资源共享，因此得到广泛的应用，已成为计算机网络技术中发展最快的分支。计算机局域网具有结构简单、投资少、数据传输速率高和可靠性高等优点。

本章主要以局域网拓扑结构、传输介质访问控制方式以及IEEE 802协议为重点介绍。另外介绍了虚拟局域网应用、无线局域网的工作原理和组网方式。

3.1　局域网概述

局域网技术是当前计算机网络技术中应用最广泛、技术发展最快的领域之一，本节对其概念、特点、功能及分类几个方面作比较全面的介绍。

3.1.1　局域网的概念

局域网(Local Area Network，LAN)是指将较小地理范围内的各种数据通信设备连接在一起的通信网络。它产生于20世纪70年代，由于微型计算机的蓬勃发展，计算机应用的迅速普及与计算机技术的提高，催生了计算机网络应用的不断深入和扩大，人们对信息交流、资源共享和高带宽产生了迫切需求，这些都直接推动着局域网的发展。

局域网具备如下属性：

(1) 局域网是一个通信网络。从OSI参考模型的协议层角度看，它仅包含了低两层(物理层和数据链路层)的功能，所以连到局域网的数据通信设备必须加上高层协议和网络软件才能组成计算机网络。

(2) 局域网连接的是数据通信设备。这里的数据通信设备是广义的，包括计算机(个人计算机、服务器等)、终端设备以及外围设备等。

(3) 局域网传输距离有限，网络覆盖的范围小。

3.1.2 局域网的特点

局域网的属性决定了它与广域网（WAN）不同，它一般限制在一定距离区域内。一般所说的局域网是指以微机为主组成的局域网，具有以下主要特点。

（1）通信速率较高。局域网络通信传输率的单位为兆比特每秒（Mbps），一般是10Mbps～100Mbps，最高可达1000Mbps。

（2）通信质量较好，传输误码率低，传输延迟小。局域网误码率为10^{-10}～10^{-6}，延迟在几十毫秒之内。

（3）通常属于某一单位、部门、学校或企业。局域网的范围一般在2.5km之内。

（4）支持多种通信传输介质。局域网中可使用多种通信介质，如电缆（细缆、粗缆、双绞线）、光纤及无线传输等。

（5）局域网组网成本低。局域网一般以价格低而功能强的微机为主。

（6）局域网的安装较简单，可扩充性好。目前，局域网主要采用以集线器为中心的星形网络结构，扩充服务器、工作站等十分方便，某些站点出现故障时整个网络仍可以正常工作。

（7）如果采用宽带局域网，则可以实现数据、语音和图像的综合传输。

3.1.3 局域网的功能和分类

1. 局域网的功能

局域网最主要的功能是提供资源共享和相互通信，它可提供以下几项主要服务。

（1）资源共享。包括硬件资源共享、软件资源共享及数据库共享。在局域网上各用户可以共享昂贵的硬件资源，如大型外部存储器、绘图仪、激光打印机和图文扫描仪等特殊外设。用户可共享网络上的系统软件和应用软件，避免重复投资及重复劳动。网络技术使大量分散的数据能被迅速集中、分析和处理，分散在网内的计算机用户可以共享网内的大型数据库而不必重新设计这些数据库。

（2）数据传送和电子邮件。数据和文件的传送是网络的重要功能，局域网不仅能传送文件和数据信息，还可以传送声音和图像。局域网站点之间可提供电子邮件服务。

（3）提高计算机系统的可靠性。局域网中的计算机可以互为后备，避免了单机系统无后备时可能由于故障导致系统瘫痪的情况，大大提高了系统的可靠性，特别在工业过程控制、实时数据处理等应用中尤为重要。

（4）易于分布处理。局域网可以将多台计算机连成高性能的计算机系统，通过一定的算法，将较大型的综合性问题分给不同的计算机去完成。在网络上可建立分布式数据库系统，使整个计算机系统的性能大大提高。

2. 局域网的分类

局域网有多种不同的分类方法，如按拓扑结构分类、按传输介质分类、按介质访问控

制方法分类等。

(1) 按拓扑结构分类。前面网络体系结构中已介绍了几种常见的网络拓扑,在局域网中按不同的拓扑结构可以组建总线形、星形、环形和树形局域网等。

(2) 按传输介质分类。局域网使用的主要传输介质有双绞线、细同轴电缆和光缆等。

(3) 按介质访问控制方法分类。介质访问控制方法提供传输介质上网络数据传输的控制机制。按不同的介质访问控制方式,局域网可分为以太网和令牌环网等。

(4) 按网络使用的技术分类。可将局域网分为以太网、ATM 网、快速以太网和FDDI 网等。

3.2 局域网体系结构

在第 2 章中讲解了开放系统互连参考模型(OSI/RM)的体系结构,它为局域网的标准化工作提供了良好的基础和经验。虽然局域网只是计算机网络的一个分支,但由于其自身的特性,使得它与广域网有很多区别,IEEE 802 局域网参考模型与 OSI 参考模型也有所不同,如图 3-1 所示。

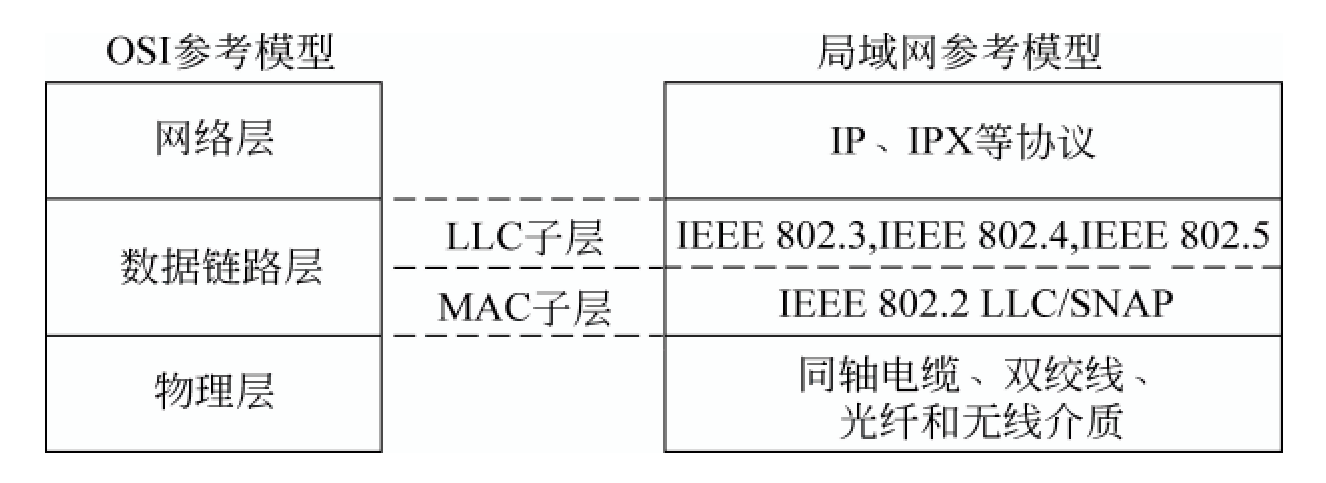


图 3-1 IEEE 802 局域网参考模型

3.2.1 局域网参考模型

局域网参考模型只对应 OSI 参考模型的数据链路层与物理层,它将数据链路层划分为两个子层:逻辑链路控制(Logical Link Control,LLC)子层与介质访问控制(Media Access Control,MAC)子层。

(1) 物理层。物理层涉及通信在信道上传输的比特流,它的主要作用是确保二进制位信号的正确传输,包括位流的正确传送和正确接收。

(2) MAC 子层。MAC 是数据链路层的一个功能子层。它构成了数据链路层的下半部分,直接与物理层相邻。

MAC 子层主要控制、管理和分配信道的协议规范,提供多种介质访问控制方式。MAC 子层是与传输介质有关的一个数据链路层的功能子层。它的主要功能是进行合理的信道分配,解决信道竞争问题。它在支持 LLC 子层中完成介质访问控制功能,为竞争的用户分配信道使用权,并具有管理多链路的功能。MAC 子层为不同的物理介质定义了介质访问控制标准。目前,IEEE 802 已制定的介质访问控制标准有载波侦听多路访问

(CSMA/CD)、令牌环(Token Ring)和令牌总线(Token Bus)等。介质访问控制方法决定了局域网的主要性能,它对局域网的响应时间、吞吐量和网络利用率都有十分重要的影响。

(3) LLC子层。LLC也是数据链路层的一个功能子层。它构成了数据链路层的上半部分,与网络层和MAC子层相邻。

LLC子层在MAC子层的支持下向网络层提供服务。可运行于所有IEEE 802局域网协议之上的数据链路层协议被称为逻辑链路控制(LLC)。LLC子层与传输介质无关,它独立于介质访问控制方法,隐藏了各种IEEE 802网络之间的差别,向网络层提供一个统一的格式和接口。LLC子层的作用是在MAC子层提供的介质访问控制和物理层提供的比特服务的基础上,将不可靠的信道处理为可靠的信道,确保数据帧的正确传输。LLC子层的具体功能包括数据帧的组装与拆卸、帧的发送、差错控制、数据流控制和发送顺序控制等,并为网络层提供两种类型的服务:面向连接服务和无连接服务。

3.2.2 IEEE 802标准概述

为实现网络设备之间的兼容性、互换性和互操作性,以便让用户更灵活地进行设备选型,国际标准化组织开展了局域网的标准化工作。1980年2月成立了局域网标准化委员会,即IEEE 802委员会(也称为LAN/MAN Standards Committee,LMSC,即局域网/广域网标准委员会)。该委员会制定了一系列局域网标准,称为IEEE 802标准。该委员会随后于1985年公布了IEEE 802标准的5项标准文本,同年被美国国家标准局(ANSI)采纳作为美国国家标准。后来,国际标准化组织(ISO)经过讨论,建议将IEEE 802标准定为局域网国际标准,也称为以太网(Ethernet)标准。

IEEE 802标准仅包含OSI参考模型的物理层和数据链路层协议,其他较高层次的协议目前还没有制定,一般会参考使用OSI参考模型和其他的相应标准(如TCP/IP)。IEEE 802已增加到多个分委员会,各分委员会的结构关系如图3-2所示。

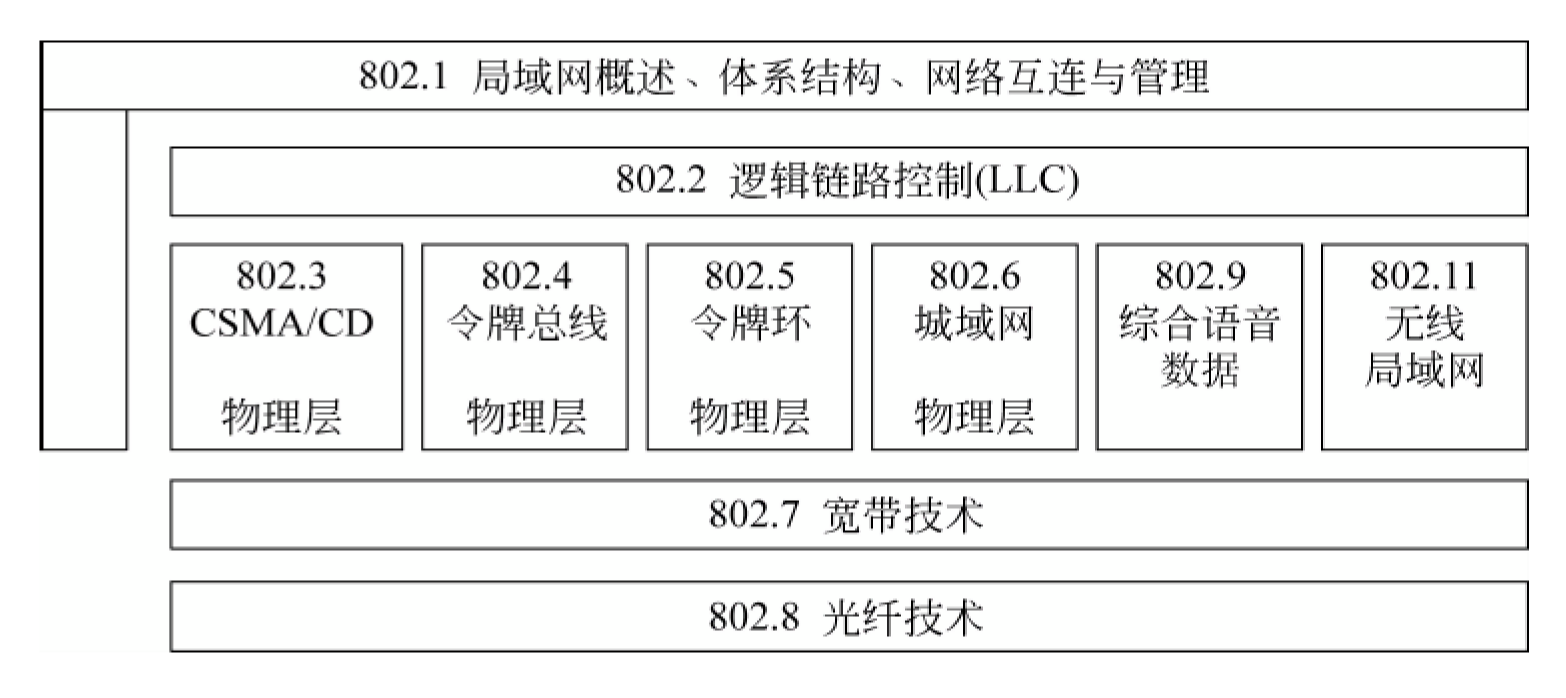


图3-2 IEEE 802各分委员会的结构关系

同时,IEEE 802委员会为局域网制定了一系列标准规则,如表3-1所示。

表 3-1 IEEE 802 标准

IEEE 802 分委员会名	制定的局域网标准
IEEE 802.1	局域网概述、体系结构、网络管理和网络互连
IEEE 802.2	逻辑链路控制(LLC)
IEEE 802.3	CSMA/CD 访问方法和物理层规范
IEEE 802.4	Token Passing BUS(令牌总线)
IEEE 802.5	Token Ring(令牌环)访问方法和物理层规范
IEEE 802.6	城域网访问方法和物理层规范
IEEE 802.7	宽带技术咨询和物理层规范
IEEE 802.8	光纤技术咨询和物理层规范
IEEE 802.9	综合语音/数据服务的访问方法和物理层规范
IEEE 802.10	安全与加密访问方法和物理层规范
IEEE 802.11	无线局域网访问方法和物理层规范
IEEE 802.12	快速局域网访问方法和物理层规范
IEEE 802.14	交互式电视网
IEEE 802.15	个人无线局域网访问方法和物理层规范
IEEE 802.16	宽带无线局域网访问方法和物理层规范

3.3 传输介质访问控制方式

传输介质访问控制方式的主要内容有两个方面：一是要确定网络中每一个节点能够将信息发送到介质上的特定时刻;二是要解决如何对共享介质访问和利用加以控制。常用的介质访问控制方法有 3 种：总线结构的带冲突检测的载波侦听多路访问 CSMA/CD 方法、环形结构的令牌环(Token Ring)访问控制方法和令牌总线(Token Bus)访问控制方法。

3.3.1 信道分配

信道分配也就是介质共享技术。通常,可将信道分配方法划分为两类：静态分配方法和动态分配方法。

1. 静态分配方法

所谓静态分配方法,也是传统的分配方法,就是采用频分多路复用或时分多路复用的方法,将单个信道划分后,静态地分配给多个用户。

当用户工作站数较多,或使用信道的工作站数在不断变化,或者通信量的变化具有突发性时,静态频分多路复用性能较差。

2. 动态分配方法

所谓动态分配方法就是动态地为每个用户站点分配信道使用权，主要包括以下3种技术。

(1) 轮转：使每个用户站点轮流获得发送的机会，这种技术称为轮转。它适合于交互式终端对主机的通信。

(2) 预约：将传输介质上的时间分隔成时间片，网上用户站点若要发送，必须事先预约能占用的时间片。这种技术适用于数据流的通信。

(3) 争用：是指所有用户站点都能争用介质。它实现起来简单，对轻负载或中等负载的系统比较有效，适合于突发式通信。

争用方法属于随机访问技术，而轮转和预约的方法则属于控制访问技术。

3.3.2 载波侦听多路访问控制方法

1. CSMA/CD 工作原理

CSMA/CD(Carrier Sense Multiple Access/Collision Detect)即载波监听多路访问/冲突检测。在以太网中，传送信息以数据包为单位，简称包。在总线上如果某个工作站有数据包要发送，它在向总线上发送数据包之前，先检测一下总线是“忙”还是“闲”，如果检测的结果是“忙”，则发送站会随机延迟一段时间再去检测总线，若这时检测总线是“闲”，就可以发送数据包了。而且在数据包的发送过程中，发送站还要检测其发到总线上的数据包是否与其他站点的数据包产生了冲突，当发送站一旦检测到产生冲突，它就立即放弃本次发送，并向总线上发出一串干扰串，总线上的各站点收到此干扰串后，则放弃发送，并且所有发生冲突的节点都将按一种退避算法等待一段随机的时间，然后重新竞争发送。

从以上叙述可以看出CSMA/CD的工作流程(见图3-3)：先听后发，边发边听；测到冲突，退后再发。

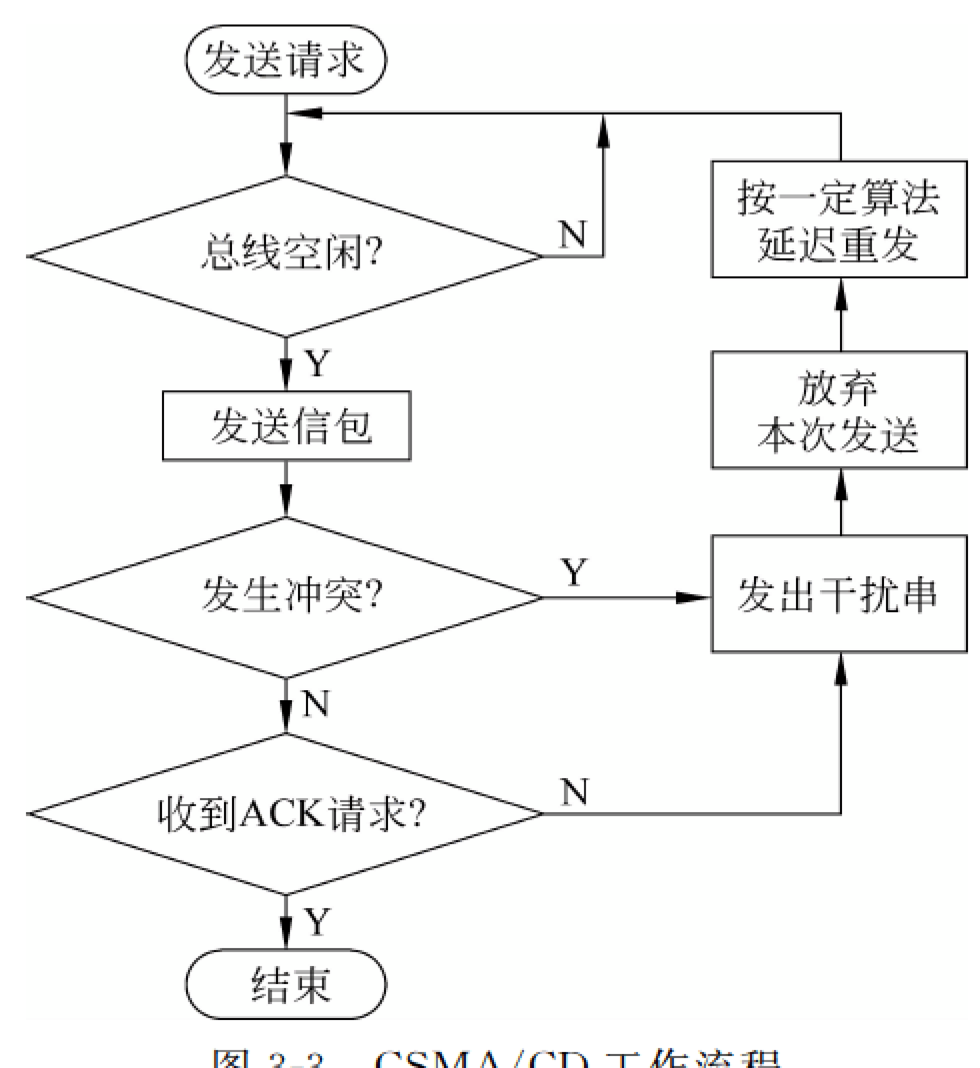


图3-3 CSMA/CD 工作流程

2. CSMA/CD 冲突检测所需的时间

在 CSMA/CD 的传输控制方式中，冲突要经过最长多少时间才被检测出来？检测冲突的时间等于总线上最远的两个站点之间端到端延迟时间 Δt 的两倍（即 $2\Delta t$）。这种 CSMA/CD 冲突检测对发送站所发送的数据包长度有一定的要求，例如，在 10Mbps 的数据速率下，其数据帧长度的最小值不能小于 64B（如所发送的信息不足时，可加以填充）。因为 CSMA/CD 的工作原理要求发送站一边发送数据一边进行冲突检测，若检测到冲突则立即终止发送，然后推迟一段时间再发送。

3.3.3 令牌环访问控制方法

1. 令牌环网工作原理

令牌环网的拓扑结构是所有节点串行连接而形成的一个封闭环路，如图 3-4 所示。环路上的某个站点要发送信息（以下简称发送站），它仅需要把信息往它的下游站点发送即可。下游站点收到信息以后，要进行地址识别，以判断该信息是否是发送给本地主机的，如果不是发送给本地主机，则该站点把信息继续转发给它的后继站点；如果是发送给本地主机，则该站点会将此信息复制给本地主机。另外，该站点接收了信息以后，对已接收信息是继续转发还是终止该数据包的传送，由环控制策略决定。由令牌环网的工作原理可以看出，当某一站点发送数据包以后，在环路上的每个站点都可以接收到这个数据包，而只有与该数据包目的地址相同的工作站才会接收该数据包，其他站点是不会接收该数据包的。另外，还可以看出，整个环形信道是由传输介质和中继器构成的，只要将数据包送至环路，数据包就会在中继转发器之间和传输介质上循环传送，直至到达目的地站点为止，并按照一定的策略将其取下。

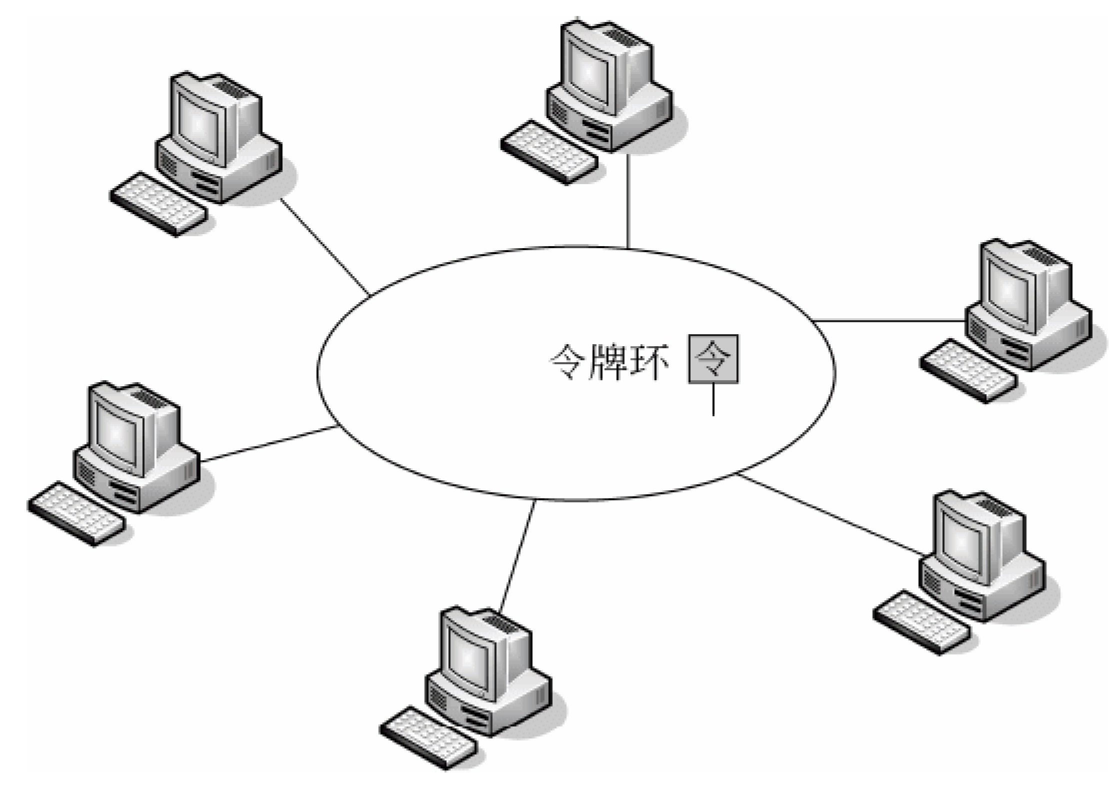


图 3-4　令牌环网

2. 令牌环网的介质访问控制方式——令牌环

令牌环技术是在环路上设置一个令牌，当所有的站点都空闲时，令牌就不停地在环形

网络上转。当某一个站点有数据包要发送,它必须等到令牌经过它时,检查令牌是否有载荷,如果获取经过的空令牌,该站点就得到了环网的使用权限。发送站点把空令牌添加数据设置成满令牌,并开始发送数据包。此时环上便没有了令牌,所有想发送信息的站点必须等待,这个数据包在环路上绕行一周又会重新回到发送站,并被发送站从环上卸载下来,同时发送站会向环上插入一个新的空令牌。一旦新的空令牌插入到环中,下游有数据发送的站点就可获得它并传输数据。

令牌环的主要优点是它提供对传输介质访问的灵活控制。而且在负载很重的情况下,这种令牌环的控制策略是高效和公平的。它的主要缺点有两个:一个是在轻负载的情况下,由于传输数据包前必须要等待一个空令牌的到来,这样造成了较低的效率;另一个是需要对令牌进行维护,一旦令牌丢失,环网便不能再运行,所以在环路上要设置一个站点作为环上的监控站点,来保证环上有且仅有一个令牌。

3.3.4 令牌总线访问控制方法

1. 令牌总线访问控制

比较总线型网络(以太网)和令牌环网可以看出:以太网的结构简单,在站点数量少时,传输速度较快。但由于采用CSMA/CD控制策略,以竞争方式随机访问传输介质,肯定会有冲突发生,且冲突数据包要重新发送,当站点超过一定数量时,网络的性能会因重发数据次数的增加而急剧下降。

令牌环网中,无论节点数有多少,都需要等待令牌空闲时才能进行通信。由于采取按位转发方式,加之对令牌的控制、监视占用部分时间,故在节点数少时,其传输速度低于以太网;但节点数量增多时,网络性能不会像以太网那样急剧下降。

综合令牌传递方式和总线形网络的优点,在物理总线结构中实现令牌传递控制方法,构成逻辑环路,这就是IEEE 802.4的令牌总线介质访问控制技术。

令牌总线网络的典型代表是美国Data Point公司研制的ARC(Attached Resource Computer)网络。

2. 令牌总线的工作原理

在令牌总线(见图3-5)中,总线上的所有站点构成逻辑环。也就是说,所有站点都按次序分配到一个逻辑地址,每个站点都知道在其之前和在其之后的站点标识,第一个站点的前趋是最后一个网络站点,而且物理上的位置与其逻辑地址无关。

一个叫做令牌的控制帧规定了访问的权利。总线上的每一个站点如有数据要发送,必须要得到令牌以后才能发送,即拥有令牌的站点被允许在指定的一段时间里访问传输介质。该站点能传输一个或多个帧,还能探询其他站点并接收响应。当该站点完成自己的工作,或是时间用完了,它要将令牌交给逻辑位置上紧接在它后面的那个站点,那个站点由此得到数据发送权。所以,常规操作包括数据传输和令牌传输。另外,不使用令牌的站点只能在总线上对探询给予响应或要求得到响应。令牌环内的站点按照逻辑地址的降

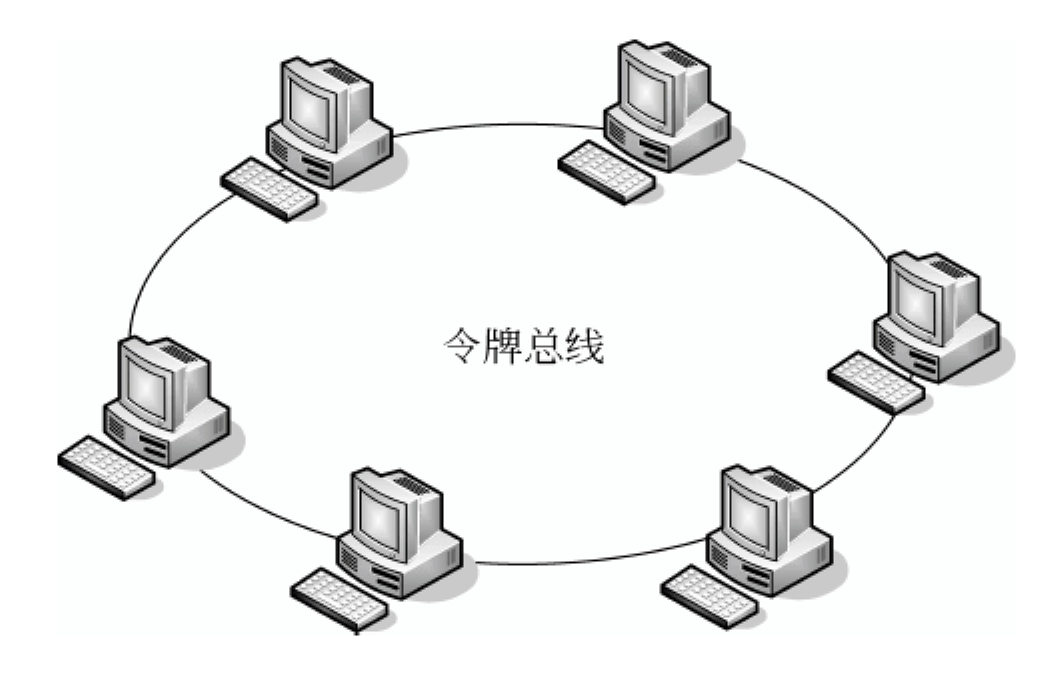


图 3-5 令牌总线网络

序排列。

3. 令牌总线的特点

由令牌总线的工作原理,不难理解令牌总线有以下特点。

(1) 不会产生传输冲突。令牌总线中,只有收到令牌的站点才能将信息发送到总线上,这样就不会像 CSMA/CD 介质访问方式那样使总线产生冲突。故令牌总线信息帧长度完全由发送信息的长短决定,没有最小分组长度要求。对于 CSMA/CD 访问控制,为使最远的站点也能检测到冲突,需要在实际的信息长度后加填充位,以满足最小长度要求。

(2) 站点有公平的访问权。获得令牌的站点,若有信息要发送即发送信息,之后将令牌传给下一站点;若没有信息发送,则立即将令牌传递到下一站点。由于站点是按初始化顺序依次接收到令牌,所以各站点都有公平的访问权。

(3) 环内传输量与传输时间可控。发送站点从发送数据帧开始到该帧发送完毕的时长,等于该帧从开始发送经环路返回发送站的时长,这个时长内数据帧的比特刚好布满环路。当全部站点都有信息发送时,等待取得令牌和发送信息的时间应等于全部令牌传送时间和发送时间的总和。

3.4 IEEE 802 与以太网

计算机网络技术的爆发式发展源于 20 世纪 80 年代,在近 40 年的发展历程中,计算机网络技术经历了发展、竞争、标准化和大发展的过程,今天人们谈起网络技术,就会提到以太网(Ethernet)技术,下面就简单介绍一下以太网与 IEEE 802 的关系。

3.4.1 以太网的产生和发展

以太网的原型是美国夏威夷大学推出的 ALOHA 网络系统,其核心思想是使用共享的公共传输信道,以广播方式实现站点与站点之间的通信。

1973 年,为了实现几台计算机之间的简单连接和信息交互,施乐公司 Palo Alto 研究

中心（PARC）的工程师麦卡夫（Robert Metcalfe）描绘出大致的网络构想，并将这项技术命名为 Ethernet（以太网），其灵感来自于“电磁辐射是可以通过发光的以太网来传播的”这一想法。当时的数据传输速率为 2.94Mbps，传输介质为宽带粗同轴电缆。

1980 年，Xerox、Intel 和 DEC 三家公司公布了以太网技术规范，也称 DIX 版以太网 1.0 版（DIX v1 或 Ethernet Ⅰ）。1982 年，该标准修改为 DIX 以太网版 2.0 规范（DIX v2 或 Ethernet Ⅱ）。今天获得广泛应用的以太网最初是由施乐（Xerox）公司创立的。

3.4.2 IEEE 802 与以太网

1980 年 IEEE 802 局域网委员会和 IEEE 计算机通信委员会通过的局部网络协议与以太网技术规范基本一致。于是，已处于局域网实用阶段的以太网技术规范成为世界范围内的第一个局部网络技术规范。当时描述的以太网的主要特征有：采用总线型拓扑结构，以标准的基带同轴电缆作为传输介质，传输速率是 10Mbps，允许节点之间的距离为 50m 等。

因此，以太网和 IEEE 802.3 协议被认为是同义词，这就是为什么今天人们讲到局域网必然要讲以太网的原因。1984 年，美国联邦政府采纳了 IEEE 802.3 标准。1985 年，IEEE 802.3 标准正式发布，名称为《IEEE 802.3 带有冲突检测的载波侦听多路访问（CSMA/CD）方法和物理层技术规范》，并在 1989 年获得了国际上的认可，被 ISO 以标准号 ISO 8802-3 采纳为 IEEE 802.3 以太网标准，以太网协议结构见图 3-6。

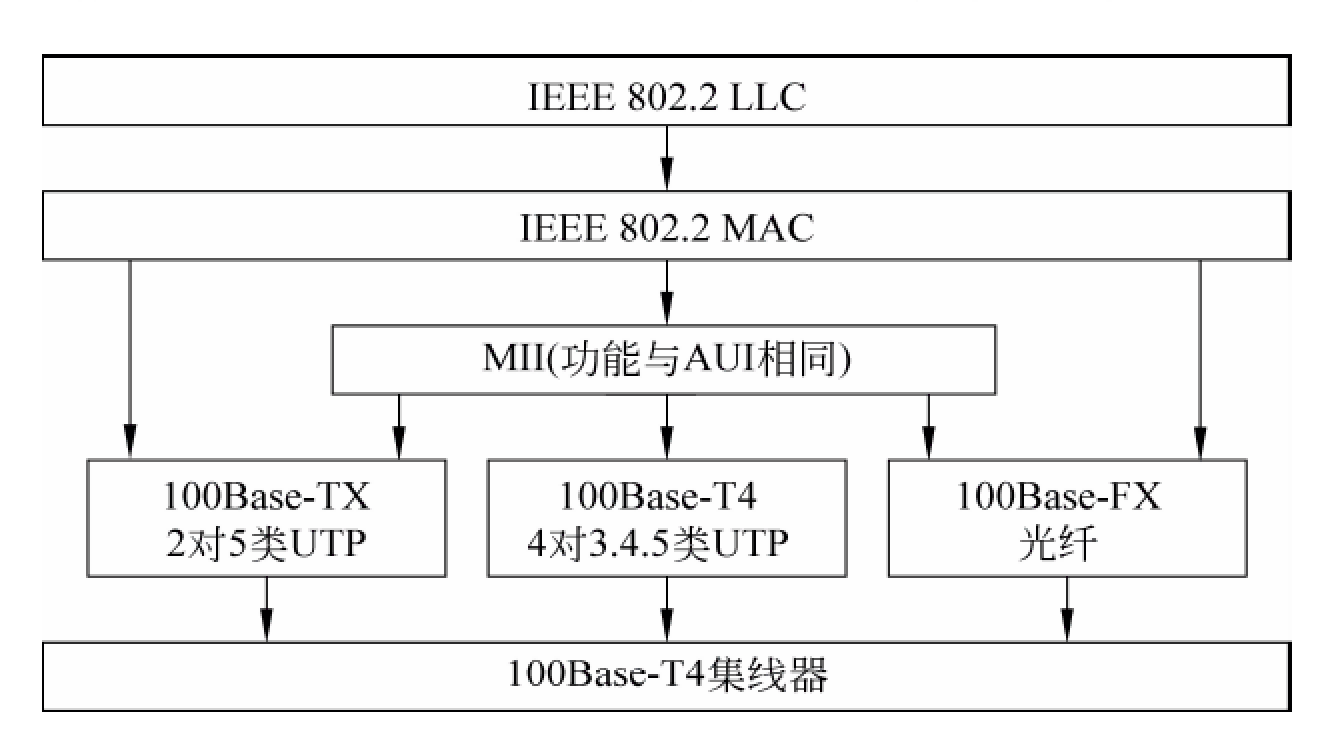


图 3-6　以太网协议结构

3.4.3 双绞线以太网

双绞线以太网是使用非屏蔽双绞线（UTP）作为传输介质的 10～100Mbps 以太网。它采用 10Base-T/100Base-T 标准，该标准与其他 IEEE 802.3 标准具有很好的兼容性，与其他传输介质间的转移相对容易。它支持结构化布线系统，采用星形拓扑结构或星形与总线形拓扑结构相结合的混合型拓扑结构，所以具有良好的故障隔离功能。网络上的每个站点通过专用的电缆与中央集线器相连，当网络上的某个电缆或者工作站出现问题时，

不会影响网络上其他站点的工作,这也使得故障诊断变得比较容易。另外,10Base-T/100Base-T 以太网较轻巧,安装密度高,特别适用于建筑物内的网络布线系统,所以使用较广泛。

10Base-T/100Base-T 以太网主要包括双绞线电缆、网卡、集线器和 RJ-45 连接器等部件,其各个部件的功能和规则如下所述。

(1) 双绞线电缆。10Base-T/100Base-T 以太网,使用具有 RJ-45 连接器,并且长度不超过 100m 的双绞线。其中,非屏蔽双绞线由包了塑料外皮的 4 对双绞线组成。为了减少线对之间的干扰,每对双绞线又由两根有规律地扭绞在一起的单股导线组成。非屏蔽双绞线直径小,重量轻,易安装,可以将串扰减至最小或是消除。

(2) 网卡。10Base-T/100Base-T 以太网需要一个含有 RJ-45 连接器的网卡,以便将双绞线的 RJ-45 连接器的接头插入到 RJ-45 插座中。

(3) 集线器。集线器的功能与中继器相似,即将信号放大整形,然后发送出去,但它能够提供更多的连接端口,端口数一般为 8、12、16、24 等。为了扩充所连接的工作站数目,可将多台集线器用级联方式连接起来,但最多只可以使用 4 个集线器 (5 个网段)。此外,大多数集线器提供了同轴电缆或者光纤接口。

(4) RJ-45 连接器。俗称水晶头,每根双绞线的两端都需压接一个 RJ-45 连接器,它有 8 个引脚,其中的引脚 1 和引脚 2 用于发送,引脚 3 和引脚 6 用于接收。

3.5 虚拟局域网

虚拟局域网(Virtual Local Area Network,VLAN),是指在交换局域网的基础上,采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个 VLAN 组成一个逻辑子网,即一个逻辑广播域,它可以覆盖多个网络设备,允许处于不同地理位置的网络用户加入到一个逻辑子网中。

近年来,随着交换局域网技术的飞速发展,交换局域网结构逐渐代替了传统局域网的共享介质结构,形成了新一代的局域网,并且交换技术的发展为虚拟局域网的实现提供了技术基础。虚拟网络技术打破了地理环境的制约,在不改动网络物理连接的情况下,可以任意将工作站在工作组或子网之间移动,工作站组成逻辑工作组或虚拟子网,能够提高信息系统的运作性能,均衡网络数据流量,合理利用硬件及信息资源。同时,利用虚拟网络技术,大大减轻了网络管理和维护工作的负担,降低网络维护费用。

虚拟网络建立在交换技术基础之上,将网络上的节点按工作性质与需要划分成若干个“逻辑工作组”,那么一个逻辑工作组就是一个虚拟网络。在传统的局域网中,通常一个网段可以是一个逻辑工作组。工作组与工作组之间通过交换机(或路由器)等互联设备交换数据。逻辑工作组的组成受到了站点所在网段物理位置的限制。逻辑工作组或物理位置的变动都需要重新进行物理连接。

虚拟局域网以软件方式实现逻辑工作组的划分与管理,逻辑工作组的站点组成不受物理位置的限制。同一逻辑工作组的成员可以不必连接在同一个物理网段上。只要以太网交换机是互连的,它们既可以连接在同一个局域网交换机上,也可以连接在不同的局域

网交换机上。当一个站点从一个逻辑工作组转移到另一个逻辑工作组时，只需要通过软件设定，而不需要改变它在网络中的物理位置。当一个站点从一个物理位置移动到另一个物理位置时，只要将该计算机连入另一台交换机，通过交换机软件设置，这台计算机还可以成为原工作组的一员。同一个逻辑工作组的站点可以分布在不同的物理网段上，但是它们之间的通信就像在同一个物理网段上一样。

3.5.1 虚拟局域网的实现技术

虚拟局域网的概念是相对于传统局域网而言的。虚拟局域网在功能和操作上与传统局域网基本相同，它与传统局域网的主要区别在于“虚拟”组成，即虚拟局域网的组网方式与传统局域网的组网方式不同。虚拟局域网组成不受节点物理位置的约束，虚拟局域网的一组节点可以位于不同的物理网段上，节点间相互间通信如同一个局域网。虚拟局域网可以跟踪节点位置的变化，当节点物理位置改变时，无须人工重新配置。因此，虚拟局域网的组网方法十分灵活。

虚拟局域网的划分可以只根据功能、部门或应用而不考虑用户的物理位置。以太网交换机的每个端口都可以分配给一个虚拟局域网。分配给同一个虚拟局域网的端口共享广播域，分配给不同的虚拟局域网的端口不共享广播域，这将全面提高网络的性能。

1. 静态虚拟局域网

静态虚拟局域网就是静态地将以太网交换机上的一些端口划分给一个虚拟局域网。这些端口一直保持这种配置关系直到人工改变它们。在虚拟局域网配置中，例如将以太网交换机端口 1、2、6 和 7 组成 VLAN1，端口 3、4、5 和 8 组成 VLAN2。

虚拟局域网既可以在单台交换机中实现，也可以跨越多台交换机。

2. 动态虚拟局域网

所谓动态虚拟局域网是指交换机上的虚拟局域网端口是动态分配的。通常，动态分配的原则以 MAC 地址、逻辑地址或数据包的协议类型为基础。如果以 MAC 地址为基础，分配虚拟局域网，网络管理员就可以通过指定某些 MAC 地址的计算机属于某一个虚拟局域网，不管这些计算机连接到哪个交换机的端口，它都属于设定的虚拟局域网。这样，如果计算机从一个位置移动到另一个位置，连接的端口从一个换到另一个，只要计算机的 MAC 地址不变，它仍将属于原虚拟局域网的成员，无须网络管理员对交换机软件进行重新配置。

3.5.2 虚拟局域网的优点

1. 减少网络管理开销

在有些情况下，由于企业部门重组和人员流动，网络需要重新配置。虚拟局域网技术

为减少网络设备重新配置提供了一个行之有效的方法。当虚拟局域网的站点从一个位置移到另一个位置时，只要它们还需要在同一个虚拟局域网中，并且仍连接到网内交换机端口，则这些站点不用重新配置。站点位置的改变，只要简单地将站点插到另一个交换机端口，并对该交换机端口进行配置即可。

2. 控制广播活动

一个虚拟局域网中的广播流量不会传输到该虚拟局域网之外，邻近的端口和虚拟局域网也不会收到其他虚拟局域网产生的任何广播信息，如图 3-7 所示。虚拟局域网越小，虚拟局域网中受广播活动影响的用户越少。这种配置方式大大地减少了广播流量，为用户的实际流量释放了带宽，弥补了局域网易受广播风暴影响的弱点。

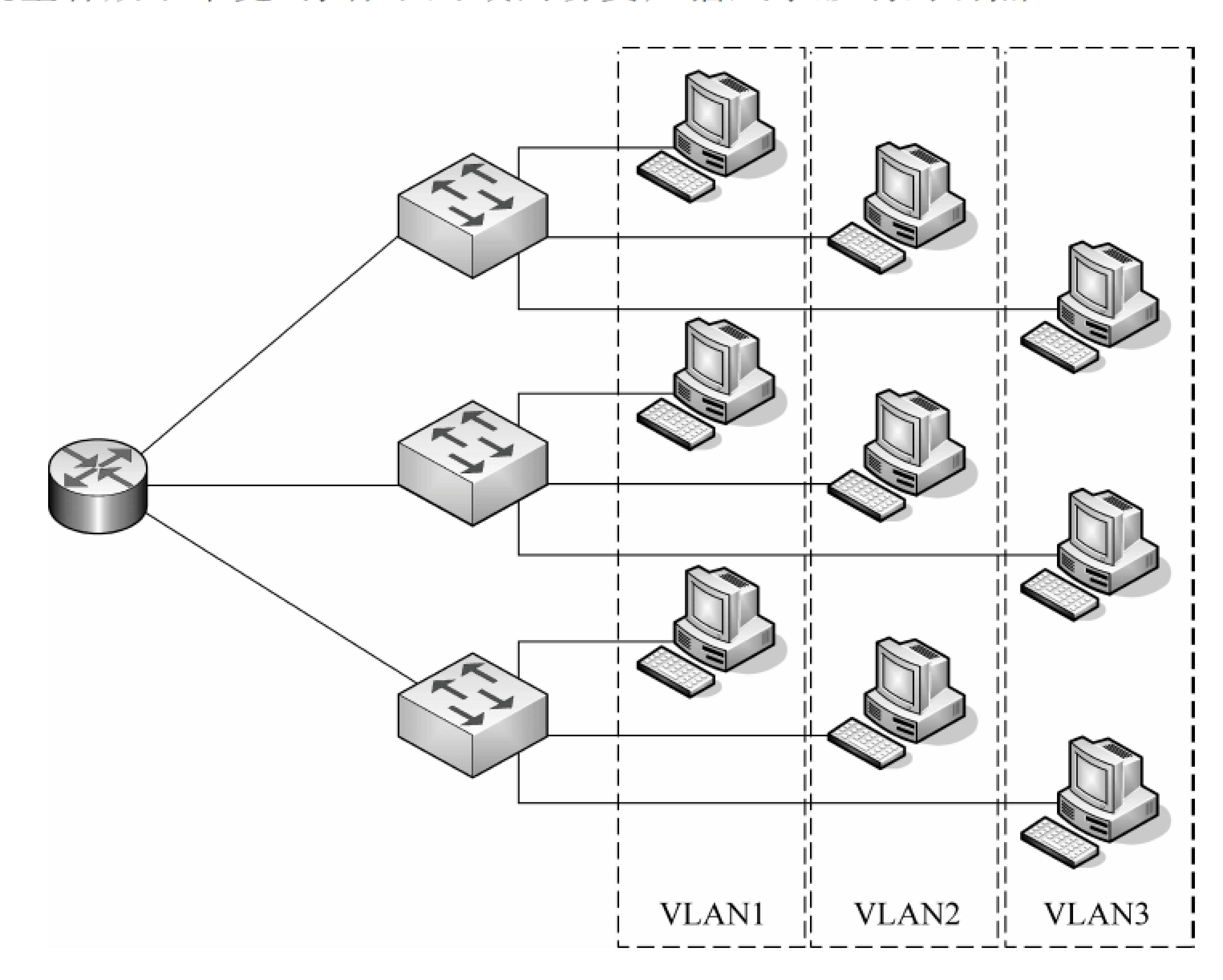


图 3-7 虚拟局域网示意图

3. 提供较好的网络安全性

在网络应用中，经常有机密和重要的数据在局域网中传递，传统的共享式以太网一个很严重的安全问题是它很容易被穿透。因为网上任一节点都需要侦听共享信道上的所有信息，所以用户通过插接到集线器的一个活动端口就可以获得该段内所有流动的信息。网络规模越大，安全性就越差。

提高安全性的一个经济实惠和易于管理的技术，就是利用虚拟局域网技术将局域网分成多个广播域。因为虚拟局域网上无论是单播信息流还是广播信息流都不会流入另一个虚拟局域网，因此，通过适当地配置虚拟局域网及该虚拟局域网与外界的连接，就可以提高网络的安全性。

3.6 无线局域网

3.6.1 无线局域网概述

随着无线局域网(Wireless Local Area Net work,WLAN)相关技术的不断进步,近年来在许多不适合网络布线的场合,无线局域网获得了广泛应用。

1. 无线局域网的定义

无线局域网是计算机网络与无线通信技术相结合的产物。无线局域网的通信方式是利用无线多址信道的一种有效方法来支持计算机之间的通信,并为局域网通信的移动化、个性化和多媒体应用提供了可能。通俗地说,无线局域网就是在不采用传统线缆的同时,提供以太网或者令牌网络的功能。

互联设备构成骨干网。利用无线接入点(Access Point,AP)来支持移动终端的移动和漫游。配有无线网卡的台式PC、笔记本电脑或其他设备就可以与无线网络连接起来。无线局域网与有线局域网的作用基本相同,就是在网络的各设备之间传送分组信息。不同的是,无线局域网中所用的是便携设备,其中的分组传输包括移动站之间及移动站与固定站之间的传输。

2. 无线局域网的特点

无线局域网与传统机架布线式局域网有以下特点:

(1) 可移动性。适合于变化频繁的工作场合。

(2) 容易安装。无须布线,大大节约了建网时间。

(3) 组网灵活。即插即用,网络管理人员可以迅速将其加入到现有网络中,并在某种环境下运行。

(4) 成本低。它提供了不受线缆限制的应用,用户可以随时上网。

3. 无线局域网的主要类型

一般,凡是采用无线电波、红外线和激光等无线传输介质的局域网都可称为无线局域网。目前,无线局域网主要采用无线电波和红外线作为传输介质,还可将它进一步细分为基于无线电波的无线局域网和基于红外线的无线局域网。

在采用无线电波作为传输介质的无线局域网中,如果按照调制方式的不同,还可以进一步细分为窄带调制方式和扩展频谱方式。

(1) 基于窄带调制的无线局域网。传统的无线电系统(比如广播电台、电视台及GSM手机等)都采用窄带调制方式。在这种方式下,数据基带信号的频谱直接通过射频组件发射出去。它在一个窄的频带内集中全部功率,无线电频谱的利用率高。给予窄带频谱方式的无线局域网需要向无线电管理委员会申请专用频段。如果选用ISM频段,则可以避免申请环节,但在无线局域网附近的通信设施或者设备也适用于这一频段时,会产

生干扰，严重影响通信质量。

(2) 基于扩展频谱方式的无线局域网。跳频技术（Frequency-Hopping Spread Spectrum，FHSS）和直接序列扩频技术（Direct Sequence Spread Spectrum，DSSS）是扩展频谱技术的主要技术，这两种技术是在第二次世界大战中军队所使用的技术，为了确保通信系统的稳定性及保密性，将数据基带信号的频谱扩展至几倍到几十倍后再发射出去，它牺牲了频带带宽。

由于单位频带内的功率降低，对其他电子设备的干扰也减少了，因此提高了通信系统的抗干扰能力和安全性。另外，基于扩展频谱方式的局域网一般选择 ISM 频段。如果发射功率及带外辐射满足无线电管理委员会的要求，则无须提出专门申请。

红外线传输在无线传输领域中是一项较成熟的技术，很早就应用在各类家电的控制和信息产品的数据传输上。一个主要原因是成本较低，红外线发光二极管及接收器等元件也比射频组件便宜。

3.6.2 无线局域网的主要标准

在无线局域网技术标准中，除了 IEEE 802.llx 系列标准以外，还有欧盟推出的 Hiper LAN、UBM、Bluetooth（蓝牙）和 Home RF 等标准。目前，无线局域网国际标准为 IEEE 802.11 系列标准，中国推出的相关标准主要有 GB 15629.11 和 GB 15629.1102。

IEEE 802.11 是第一代无线局域网标准之一，也是电子与电气工程师学会（IEEE）发布的第一个无线局域网标准，是 IEEE 802.llx 系列标准的基础标准。1999 年 8 月，IEEE 802.11 标准得到了进一步的完善和修订，增加了两个补充标准，即 IEEE 802.lla 和 IEEE 802.llb。

IEEE 802.lla 扩充了标准的物理层，工作在 5.8GHz 频带，传输速率为 5Mbps、11Mbps 和 54Mbps。它采用正交频分多路复用（Orthogonal Frequency Division Multiplexing，OFDM）的独特扩频技术，可以提供 25Mbps 的无线 ATM 接口和 10Mbps 的以太网无线结构接口，能够支持语音、数据和图像等业务，完全能满足室内外的各种应用场合。

IEEE 802.llb 标准工作在 2.4GHz 频带，采用 DSSS 扩频技术和补码键控（CCK）调制方式。该标准可以提供 11Mbps 的数据速率，还能够在 1Mbps、2Mbps、5.5Mbps 和 11Mbps 等不同速率之间自动切换，从根本上改变了无线局域网的设计和应用现状，扩大了无线局域网的应用领域。目前，大多数厂商生产的无线局域网产品都基于 IEEE 802.llb 标准。此外，IEEE 在 2003 年公布了 IEEE 802.llg 标准，它不仅与目前比较普及的 IEEE 802.llb 标准保持良好的兼容性，而且具有与 IEEE 802.lla 标准相同的传输速率（高达 54Mbps）。

由于 IEEE 802.llb 标准比较普及，在此作相关的技术分析如下：IEEE 802.llb 无线局域网的带宽最高可达 11Mbps，比以前刚批准的 IEEE 802.11 标准快 5 倍，扩大了无线局域网的应用领域。另外厂商也可根据实际情况采用 5.5Mbps、2Mbps 和 1Mbps 带宽，实际的工作速度在 5Mbps 左右，与普通的 10Base-T/100Base-T 规格有线局域网几乎处

于同一水平。作为公司内部的设施，可以基本满足使用要求。IEEE 802.11b 使用的是开放的 2.4GHz 频段，不需要申请就可使用。既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱线缆的束缚，实现真正意义上的移动应用。

IEEE 802.11b 无线局域网与 IEEE 802.3 以太网的原理很类似，都是采用带载波侦听的方式来控制网络中信息的传送。不同之处是以太网采用的是 CSMA/CD 技术，网络上所有工作站都侦听网络中有无信息发送，当发现网络空闲时即发出自己的信息，如同抢答一样，只能有一台工作站抢到发言权，而其余工作站需要继续等待。如果一旦有两台以上的工作站同时发出信息，则网络中会发生冲突，冲突后信息都会丢失，各工作站则将继续抢夺发言权。而 IEEE 802.11b 无线局域网则引进了冲突避免技术，从而避免了网络中冲突的发生，可以大幅度提高网络效率。

IEEE 802.11b 标准的优点如下。

(1) 速度。2.4GHz 直接序列扩频无线电提供最大为 11Mbps 的数据传输速率，无须直线传播。

(2) 动态速率转换。当射频情况变差时，降低数据传输速率为 5.5Mbps、2Mbps 和 1Mbps。

(3) 使用范围。IEEE 802.11b 支持以百米为单位的范围。

(4) 可靠性。与以太网类似的连接协议和数据包确认提供可靠的数据传送和网络带宽的有效使用。

(5) 车用性。与以前的标准不同的是，IEEE 802.11b 只允许一种标准的信号发送技术。

(6) 电源管理。IEEE 802.11b 网络接口卡可转到休眠模式，访问点将信息缓冲到客户，延长了笔记本电脑的电池寿命。

(7) 漫游支持。当用户在楼房或公司部门之间移动时，允许在访问点之间进行无缝连接。

(8) 加载平衡。IEEE 802.11b 更改与之连接的访问点，以提高性能。

(9) 可伸缩性。最多 3 个访问点可以同时定位于有效使用范围中，支持上百个用户。

3.6.3 无线相关产品介绍

1. 无线网卡

按无线网卡采用的接口划分，有 PCI 无线网卡（包括 ISA 接口）、USB 无线网卡和 PC-MCIA 无线网卡（包括 CF 接口），如图 3-8 所示。



(a) PCI 无线局域网卡



(b) PCMCIA 无线局域网卡

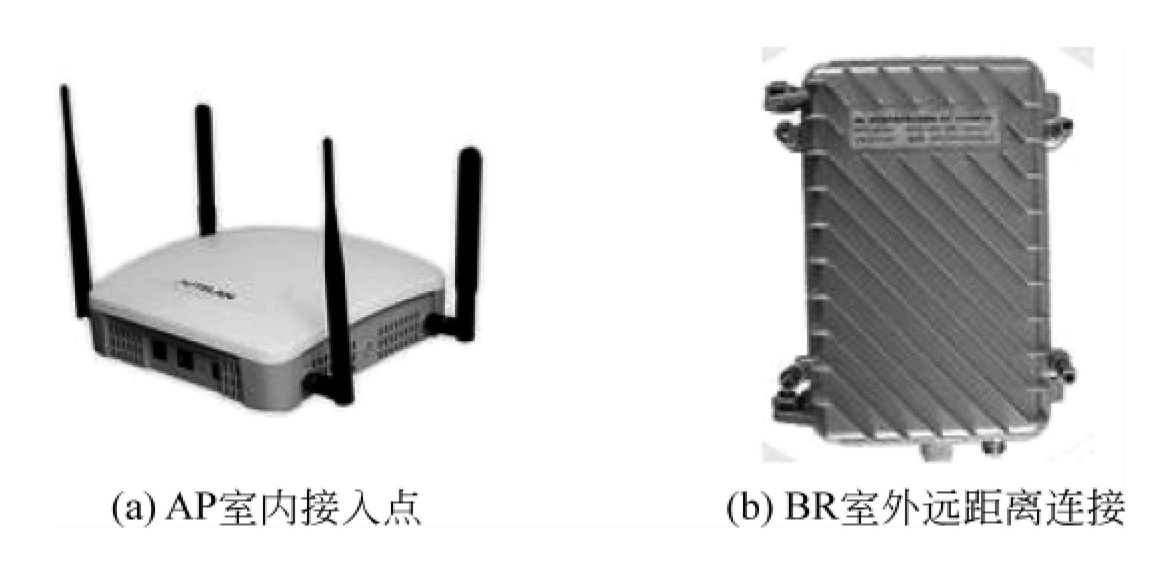


(c) USB 无线局域网卡

图 3-8 无线网卡

2. 无线接入点

无线接入点(无线 AP)作为无线网络中的一个重要设备,其性能及位置直接影响着无线网络传输信号的强弱。要想有效提高无线网络的整体性能,选好和用好无线接入点就成了不可或缺的一个重要环节,如图 3-9 所示。

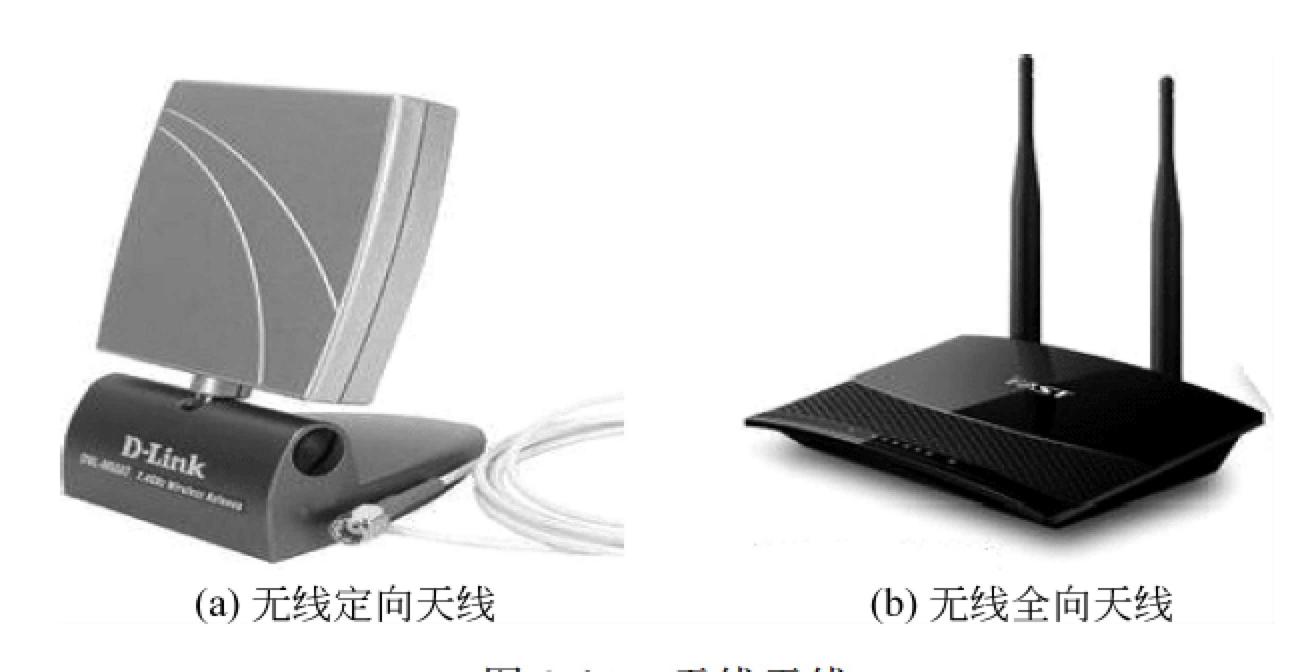


(a) AP室内接入点　　(b) BR室外远距离连接

图 3-9　无线接入点

3. 无线天线

当在室内的传输距离超出 20～30m,室外的传输距离超出 50～100m 时,就必须考虑为无线 AP 或无线网卡安装外置天线,以增强信号强度,延伸无线网络的覆盖范围。无线 AP 或无线路由器需要为无线网络内所有的无线网卡提供无线连接,因此,应当选择全向天线,如图 3-10 所示。



(a) 无线定向天线　　(b) 无线全向天线

图 3-10　无线天线

3.7　本章小结

局域网是将较小地理区域的各种数据通信设备连接在一起的通信网络。局域网的出现,使计算机网络的功能得到充分发挥,局域网是目前应用最为广泛的一类网络。本章主要介绍局域网的定义、特点与发展,各种局域网的类型及局域网的组网标准。随着用户对网络高带宽的要求,出现了各种类型的高速局域网,本章也相应地介绍了这方面的内容,同时还详细介绍了目前比较流行的虚拟局域网技术和无线局域网技术。

综合训练

一、理论题

1. 选择题

(1) 在星形局域网结构中，通常连接主机的中心接入设备是(　　)。

A. 调制解调器　　B. 交换器　　C. 路由器　　D. 集线器

(2) 对局域网来说，网络资源核心通常是(　　)。

A. 工作站　　B. 网卡　　C. 网络服务器　　D. 网络互连设备

(3) 局域网将数据链路层划分为逻辑链路控制子层与(　　)两个子层。

A. LLC　　B. 物理层　　C. MAC　　D. 网络互连层

(4) IEEE 802.3 标准是(　　)。

A. 逻辑链路控制

B. CSMA/CD 访问方法和物理层规范

C. 令牌总线访问方法和物理层规范

D. 令牌环网访问方法和物理层规范

(5) 一般局域网的数据传输速率要比广域网的数据传输速率(　　)。

A. 高　　B. 低　　C. 相同　　D. 不确定

(6) 以太网采用的标准是(　　)。

A. IEEE 802.3　　B. IEEE 802.4　　C. IEEE 802.5　　D. Token Ring

(7) 无线局域网所采用的协议为(　　)。

A. CSMA/CD　　B. Token Ring　　C. IEEE 802.11　　D. PPP

(8) 在局域网中，MAC 指的是(　　)。

A. 逻辑链路控制子层　　B. 介质访问控制子层

C. 物理层　　D. 数据链路层

2. 填空题

(1) 局域网中的数据通信被限制在________的地理范围内，能够使用具有________传输速率的物理信道，并且具有________的误码率。

(2) IEEE 802 参考模型只对应 OSI 参考模型的________层与________层。

(3) 局域网将________层划分为________子层与________子层。

(4) 以太网最大的特性在于信号是以________的方式在介质中传播。

(5) 以太网的核心技术是它的 CSMA/CD 方法，即________方法。

(6) CSMA/CD 的发送流程可以简单地概括为________，________，________，________。

(7) 动态虚拟局域网是指交换机上的________是动态分配的。

（8）无线局域网主要分为基于________的无线局域网和基于________的无线局域网。

3. 简答题

（1）什么是局域网？局域网有什么特点？
（2）IEEE 802标准规定了哪些层次？
（3）局域网的拓扑结构分为几种？每种拓扑结构具有什么特点？
（4）简述载波侦听多路访问/冲突检测(CSMA/CD)的工作原理。
（5）什么是虚拟局域网？它有什么特点？
（6）无线局域网具有哪些特点？无线局域网包括哪些设备？

二、实践题

1. 局域网打印机共享设置

参考步骤如下：

第一步，局域网共享打印机服务端设置（以Windows 7为例）。

（1）在计算机桌面右击“计算机”，在快捷菜单中选择“管理”命令，如图3-11所示。

（2）在弹出的“计算机管理”窗口中选择Guest用户，如图3-12所示。

（3）双击Guest，打开“Guest属性”窗口，确保账户不被禁用，如图3-13所示。

（4）打开服务端计算机的控制面板，选择“硬件和声音”下的“查看设备和打印机”，如图3-14所示。



图3-11　计算机管理

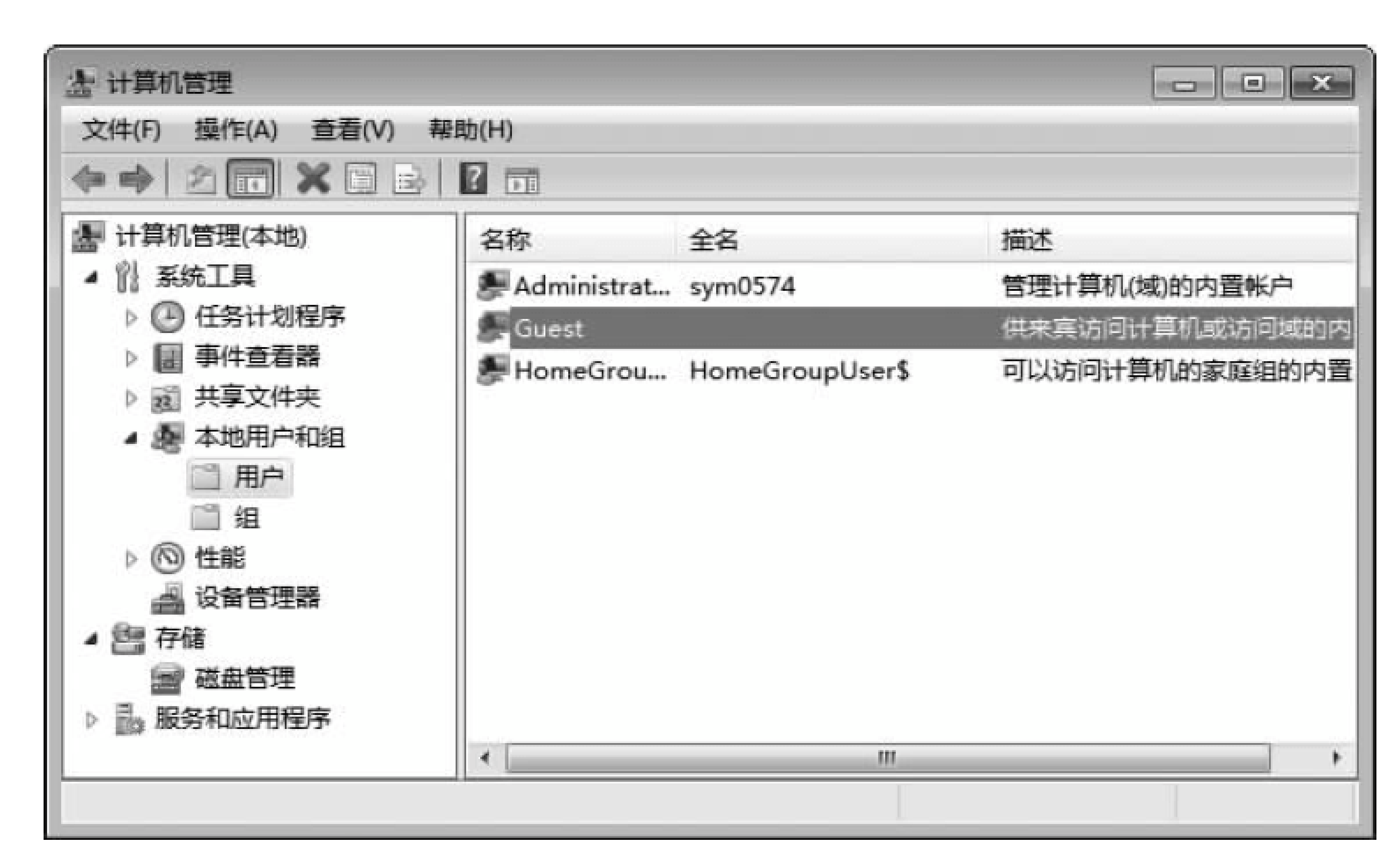


图3-12　选择Guest用户



图 3-13　开启 Guest 用户



图 3-14　查看设备和打印机

(5) 在弹出的窗口中选择共享的打印机，右击该打印机，在快捷菜单中选择“打印机属性”命令，如图 3-15 所示。

(6) 在打印机的属性对话框中，打开“共享”选项卡，勾选“共享这台打印机”，如图 3-16 所示。

(7) 打开控制面板，单击“选择家庭组和共享选项”，创建“家庭网络”，如图 3-17 所示。



图 3-15 打印机属性

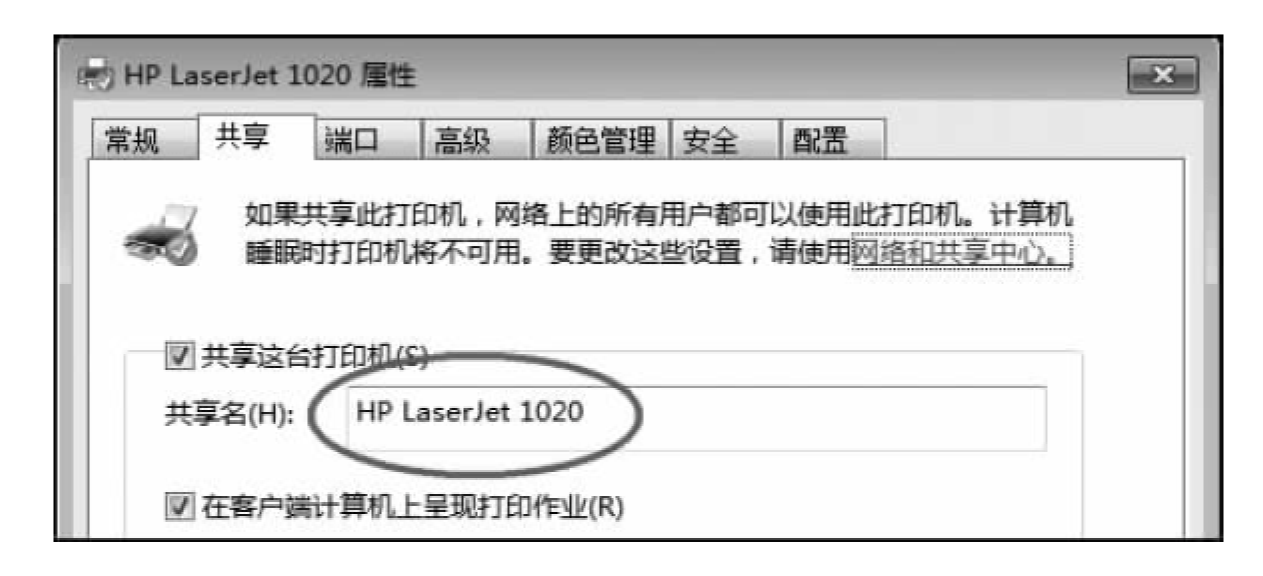


图 3-16 共享打印机



图 3-17 家庭网络

（8）打开"打开网络和共享中心"，单击"高级共享设置"，选择"启用文件和打印机共享"，如图 3-18 所示。

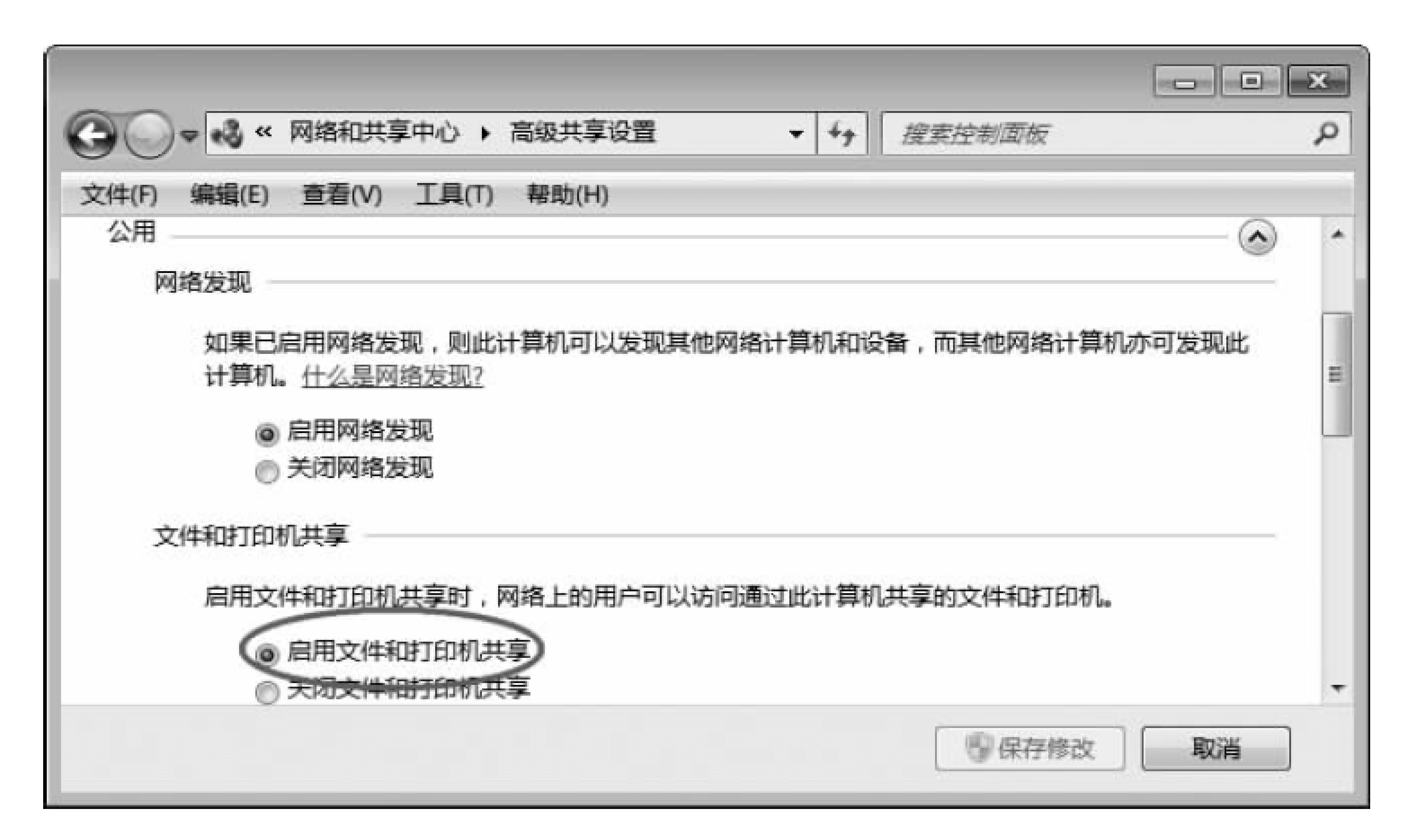


图 3-18　启用文件和打印共享

第二步，局域网共享打印机客户端配置（以 Windows XP 为例）。

（1）选择"开始"→"设置"→"打印机和传真"，在弹出的"打印机和传真"窗口中选择"添加打印机"，出现"添加打印机向导"对话框，如图 3-19 所示。



图 3-19　添加打印机

(2) 选择“网络打印机或连接到其他计算机的打印机”单选按钮，如图 3-20 所示。

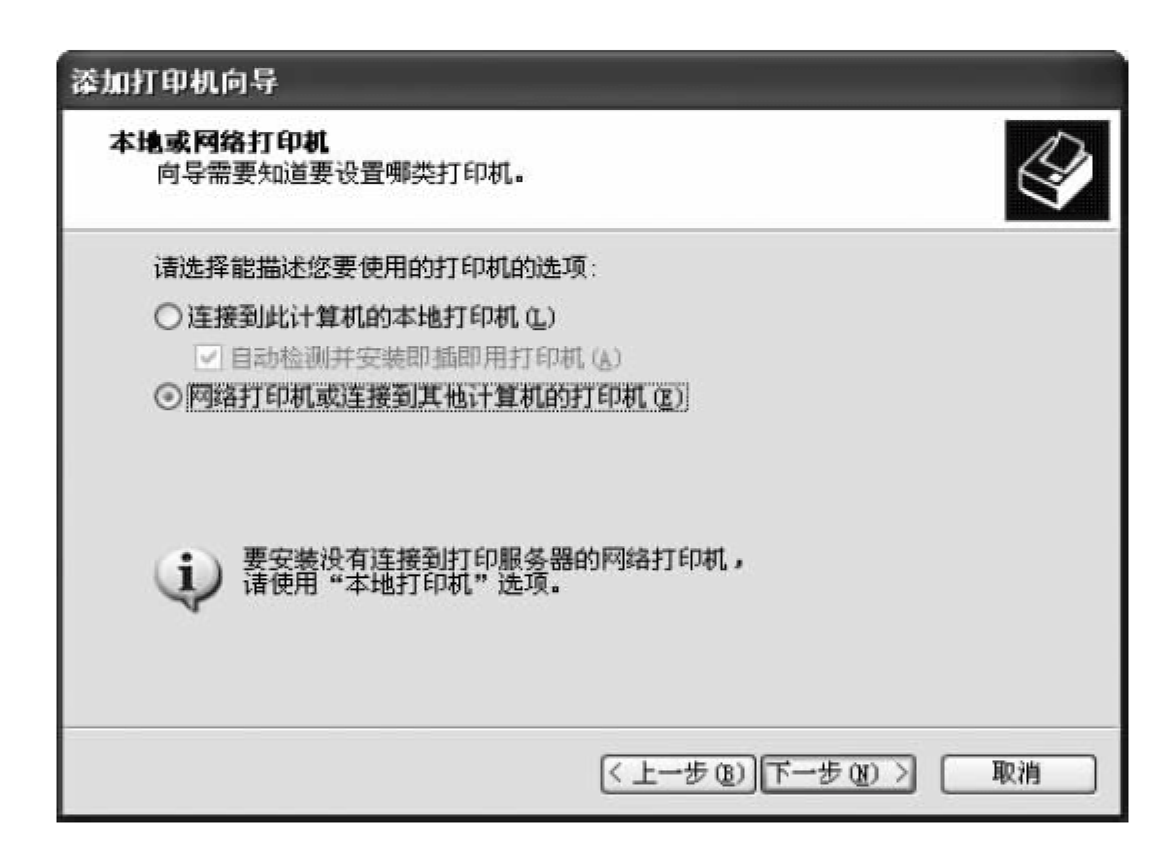


图 3-20　添加网络打印机

(3) 选择共享网络中的网络打印机，如图 3-21 所示。



图 3-21　选择共享的网络打印机

(4) 在控制面板的“打印机和传真”窗口中查看新添加的打印机，如图 3-22 所示。



图 3-22　新添加的打印机

2. 家用路由器设置

参考步骤如下：

(1) 以 TP-LINK 设备为例，在浏览器中输入 192.168.1.1，连接设备后输入用户名和密码，一般都是 admin，如图 3-23 所示。



图 3-23 登录界面

(2) 登录设备后，在窗体左侧的菜单列表中选择“设置向导”，如图 3-24 所示。



图 3-24 设置向导

(3) 选择“ADSL 虚拟拨号”单选按钮，如图 3-25 所示。

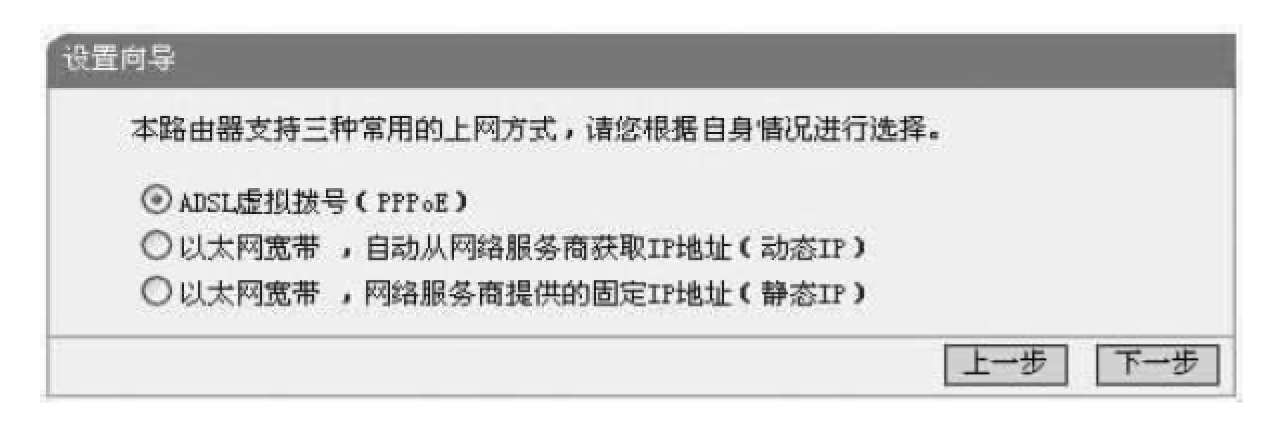


图 3-25 ADSL 虚拟拨号

（4）输入 ISP 提供的“上网账号”与“上网口令”，如图 3-26 所示。



图 3-26 输入上网账号和口令信息

（5）家用路由器设置完成，如图 3-27 所示。

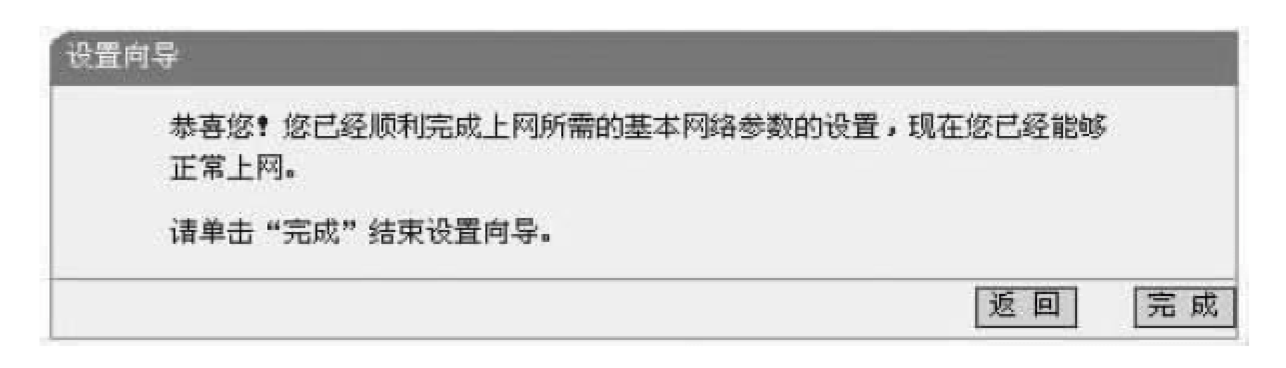


图 3-27 ADSL 自动拨号设置完成

（6）如果家庭有多台计算机上网，可以设置路由器自动分配 IP 地址。在菜单列表中选择“DHCP 服务器”，选择“启用”DHCP 服务器，根据上网计算机数量，确定自动分配 IP 地址范围，如图 3-28 所示。

DHCP服务

本路由器内建DHCP服务器，它能自动替您配置局域网中各计算机的TCP/IP协议。

DHCP服务器： 不启用 启用
地址池开始地址： 192.168.1.100
地址池结束地址： 192.168.1.107
地址租期： 120 分钟（1～2880分钟，缺省为120分钟）
网关： 0.0.0.0 （可选）
缺省域名： （可选）
主DNS服务器： 0.0.0.0 （可选）
备用DNS服务器： 0.0.0.0 （可选）

保 存 帮 助

图 3-28 启动 DHCP 服

第 4 章　网络数据通信基础

本章主要内容

- 通信的基本概念与主要技术指标
- 数据通信的基本方式
- 信号传输的复用技术
- 信号传输的差错控制

数据通信(data communication)是通信技术和计算机技术相结合而产生的一种新的通信方式,它在计算机网络中占有十分重要的地位,数据通信一般指通过各种不同的方式和传输介质,把处在不同位置的终端和计算机或计算机和计算机连接起来,从而完成数据传输、信息交换和通信处理等任务。

本章从介绍数据通信基本概念与主要技术指标入手,简要介绍数据通信的基本工作方式、信号传输的复用技术以及差错控制等内容,以使学习者掌握网络数据通信的基础知识。

4.1　数据通信基本概念

数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。因此,要理解和掌握网络数据通信知识,就必须先了解最基本的数据通信术语。

4.1.1　基本术语

1. 数据

在计算机科学中,数据(data)是指所有能输入到计算机并被计算机程序处理的符号和量,是用于输入电子计算机进行处理,具有一定意义的数字、字母、符号和模拟量等的通称。数据可分为模拟数据和数字数据两大类:模拟数据是在某个区间内连续变化的值,如声音和视频都是幅度连续变化的波形,又如温度和压力也都是连续变化的值;数字数据是离散的值,例如文本信息和整数。

对数据进行分类时,采用不同的分类方法,就会有不同的分类结果。

按性质分,可分为定位的各种坐标数据;定性的表示事物属性的数据,如山川、河流、道路等;定量的反映事物数量特征的数据,如长度、面积、体积等几何量或重量、速度等物理量;定时的反映事物时间特性的数据,如年、月、日、时、分、秒等。

按表现形式可分为数字数据,如各种统计或量测数据;模拟数据,由连续函数组成,是

指在某个区间连续变化的物理量,又可以分为图形数据(如点、线、面)、符号数据、文字数据和图像数据等,如声音的大小和温度的变化等。

按记录方式分为地图、表格、影像、磁带、纸带等。

按数字化方式分为矢量数据、格网数据等。

总而言之,数据可定义为有意义的实体,它涉及事物的存在形式。

2. 信号

信号(signal)是运载消息的工具,是消息的载体,是数据的电子或电磁编码。从广义上讲,它包含光信号、声信号和电信号等。对应于模拟数据和数字数据,信号也可分为模拟信号和数字信号,如图 4-1 所示。

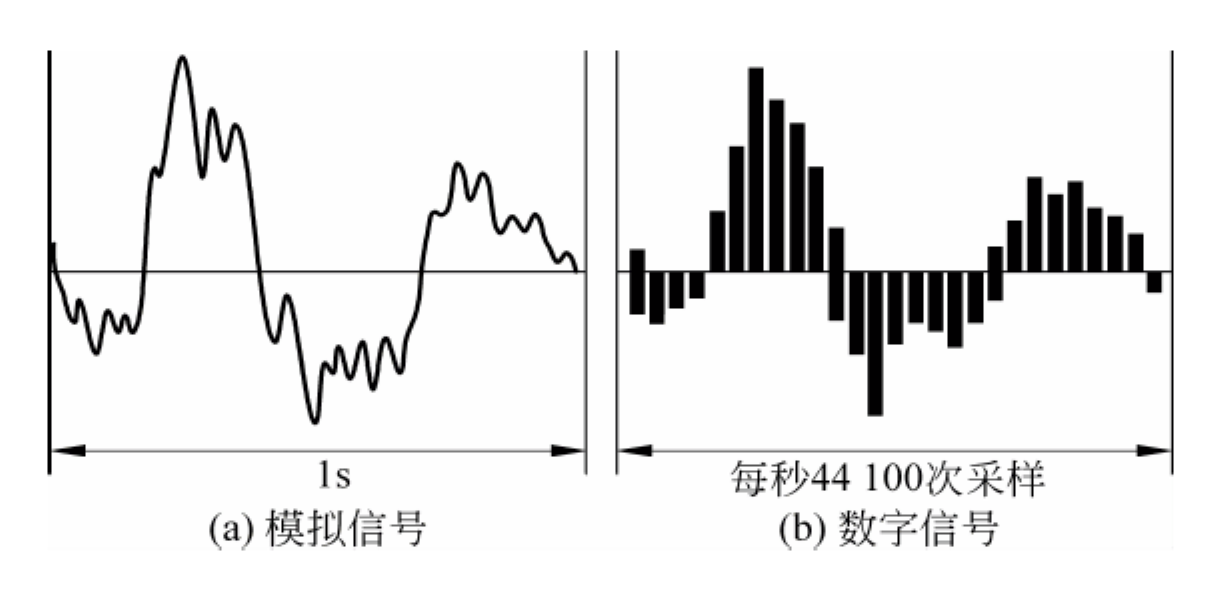


图 4-1　模拟信号和数字信号

模拟信号(analog signal)是随时间连续变化的电流、电压或电磁波,可以利用其某个参量(如幅度、频率或相位等)来表示要传输的数据。

数字信号(figure signal)则是一系列离散的电脉冲,可以利用其某一瞬间的状态来表示要传输的数据。

3. 信息

信息(information)是对客观世界中各种事物的运动状态和变化的反映,是客观事物之间相互联系和相互作用的衡量,表现的是客观事物运动状态和变化的实质内容,它能够通过文字、图像、声音、符号和数据等为人类获知的知识。一般来说,信息是指与客观事物相联系,反映客观事物的运动状态,通过一定的介质载体被发出、传递和感受,对接收对象的思维产生影响并用来指导接受对象的行为的一种描述。从本质上说,信息是反映现实世界的运动、发展和变化状态及规律的信号与消息。需要注意的是,信息具有客观性、适用性、可传输性和共享性等特征,它不随载体的物理形式的改变而改变。

信息、数据和信号三者间的关系如图 4-2 所示。

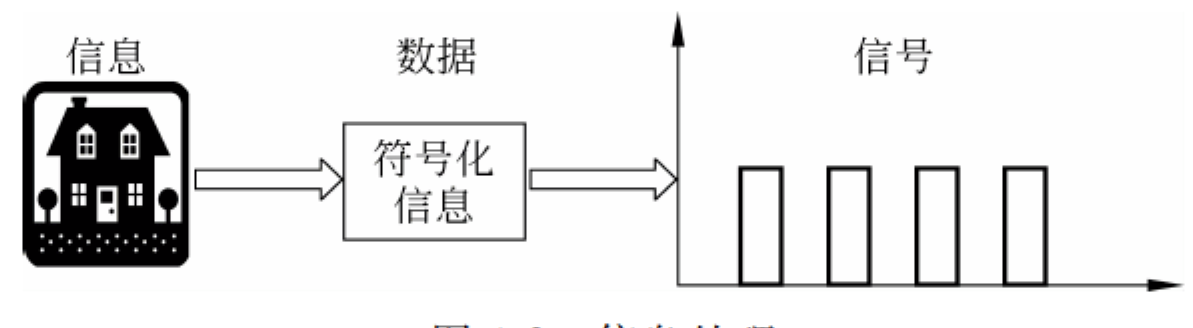


图 4-2　信息处理

4. 码元与码字

码元，也称为码位，是对计算机网络传送的二进制数字中的每一位的通称。而由若干个码元序列表示的数据单元代码通常称为码字。

例如，二进制数字 1000001 是由 7 个码元组成的序列，可以视为一个码字。在 7 位的 ASCII 码中，这个码字表示字母 A。

5. 带宽

带宽(bandwidth)通常指信道在传输信号不失真情况下的频带宽带，它指的是网络信号可使用的最高频率与最低频率之差，或者说是频带的宽度，也就是所谓的信道带宽。

例如，一条传输线路可以接受 600～2200Hz 的频率，则该传输线路所传送频率的带宽是 1600Hz。

带宽越大，所能达到的传输速率就越大，所以信道的带宽是衡量传输系统的一个重要指标。

6. 数据传输

数据传输(data transmission)是指通信双方依照通信规则，在一条或多条链路上实现双方之间传送数据的过程。数据传输按被传输的数据信号的特点可分为基带传输、频带传输和数字数据传输，按数据传输的顺序可分为并行传输和串行传输，按数据传输的同步方式可分为同步传输和异步传输，按数据传输的流向和时间可分为单工、半双工和全双工传输。

4.1.2 信息系统三要素

数据通信系统的基本通信模型是：产生和发送信息的一端叫信源，接收信息的一端叫信宿。信源经过信道到达信宿。通信系统三要素是信源、信道和信宿，三者间的关系如图 4-3 所示。

图 4-3 信源、信道和信宿

1. 信源

信源(source)就是信息的来源，可以是人、机器和自然界的物体等。信源发出信息的时候，一般以某种信息的方式表现出来，可以是符号，如文字、语音、图像和声响等，也可以是信号。

2. 信宿

信宿(sink)相对于信源而言，是信息的目的地。信宿是信息动态运行一个周期的最终环节，其功能是接收信息，并选择对自身有用的信息加以利用，直接或间接地为某一目的服务。信宿可以把信息资源转化为人类的巨大物质财富，在信息的再生产过程中，还可

以起到巨大的反馈作用。

3. 信道

信道(channel)是信号的传输通道,按传输媒介可分为有线信道和无线信道两类。有线信道包括明线(也称电缆)、同轴电缆及光缆等;无线信道有短波、超短波或微波、人造卫星、红外线以及各种散射信道等。

信息传输时必须经过一条通路,但是,一条传输介质上可以逻辑分割多条信道(即信道多路复用技术),因此,信道还可以按复用技术划分为物理信道与逻辑信道。

按传输信号类型信道可分为传输模拟信号的模拟信道和传输数字信号的数字信道。数字信号经过数/模转换后可以在模拟信道上传输,模拟信号经过模/数转换后可以在数字信道上传输。

在模拟信道中,人们一般采用“带宽”表示信道传输信息的能力,即传送信息信号的高频率与低频率之差,单位为 Hz、kHz、MHz 或 GHz。例如,电话信道的带宽为 300～3400Hz。

在数字信道中,通常用“数据传输速率”表示信道传输信息的能力,即每秒传输的比特数,单位为 bps、kbps、Mbps 或 Gbps。例如,调制解调器的传输速率为 14.4kbps、28.8kbps 或 64kbps 等。

由于带宽与数据传输速率这两个名词都是用来说明信道传输能力的,所以,在一些有关计算机网络技术的文献中,两者经常混用。但是,从技术角度讲,它们是两个完全不同的概念,应注意区别。

4.2 数据通信主要指标

在数据通信时衡量数据传输的质量指标有两个:一个是有效性,另一个是可靠性。

在目前的技术条件下,传输电缆不可能达到十分理想,再加上传输过程中遇到的各种干扰,以及信号失真等方面的原因,传输中产生错误几乎是不可避免的。虽然不可能完全避免传输过程中的差错,但是,总希望做到传输中出现的错误越少越好。要提高数据传输的质量,就要从提高有效性和可靠性的方法入手。

4.2.1 有效性

1. 数据传输速率

数据传输速率(Data Transfer Rate)是指单位时间内信道上所能传输的数据量。数字信号传输速率在数值上等于每秒钟传输的二进制比特数,单位为比特/秒(b/s,也记做 bps),又称比特率。

数据传输速率计算公式如下:

$$S = \frac{1}{T} \cdot \log_2 N(\text{bps})$$

其中：

T 为一个数字脉冲信号的宽度或重复周期，单位为秒。

N 表示一个脉冲所能表示的有效值状态，通常 $N=2^K$（K 为二进制信息的位数）。当 $N=2$ 时（数字信号，两个码元 0 与 1），数据传输速率的公式就可简化为

$$S = \frac{1}{T}$$

模拟信号传输过程中的调制速率称为波特率，也称波形速率，是指从调制解调器输出的调制信号每秒钟载波调制状态改变的次数。可以说，在数据传输过程中，线路上每秒钟传送的波形个数就是波特率，其单位为波特（baud）。若以 T（秒）表示波形的持续时间，则调制速率（B）可以表示为

$$B = S/\log_2 N(\text{Baud})$$

2. 信道容量

信道容量（channel capacity）衡量一个信道传输数据的能力，单位也用位/秒（bps）。信道容量与数据传输速率的区别在于，前者表示信道的最大数据传输速率，是信道传输数据能力的极限，而后者则表示实际的数据传输速率。这就像公路上的最大限速值与汽车实际速度之间的关系一样，它们虽然采用相同的单位，但衡量的性能指标有不同的含义。

奈奎斯特（Nyquist）首先给出了无噪声情况下码元速率的极限值 B 与信道带宽 W 的关系：

$$B = 2W(\text{Baud})$$

其中，W 是信道的带宽，也称频率范围，即信道能传输的上、下限频率的差值，单位为 Hz。由此可推出衡量信道数据传输能力的奈奎斯特公式：

$$C = 2W\log_2 N(\text{bps})$$

此处，N 仍然表示携带数据的码元可能取的离散值的个数，C 是该信道最大的数据传输速率。

由以上两式可见，对于特定的信道，其码元速率不可能超过信道带宽的两倍，但若能提高每个码元可能取的离散值的个数，则数据传输速率便可成倍提高。

例如，普通电话线路的带宽约为 3kHz，则其码元速率的极限值为 6kBaud。若每个码元可能取的离散值的个数为 16（即 $N=16$），则最大数据传输速率可达 $C=2\times3\times\log_2 16=24\text{kbps}$。

实际的信道总要受到各种噪声的干扰，香农（Shannon）则进一步研究了受随机噪声干扰的信道的情况，给出了计算信道容量的香农公式：

$$C = W\log_2(1+S/N)(\text{bps})$$

其中，S 表示信号功率，N 为噪声功率，S/N 则为信噪比。由于实际使用信道的信噪比都足够大，故常表示成 $10\log_{10}(S/N)$，以分贝（dB）为单位来计量，在使用时要特别注意。

例如，信噪比为 30dB，带宽为 3kHz 的信道的最大数据传输速率为

$$C = 3\times\log_2(1+10\log_{10}(S/N)) = 3\times\log_2(1+10^3) = 30\text{kbps}$$

由此可见，只要提高信道的信噪比，便可提高信道的最大数据传输速率。

需要强调的是，上述两个公式计算得到的只是信道数据传输速率的极限值，实际使用时必须留有充足的余地。

4.2.2 可靠性

1. 误码率

误码率(error rate)是衡量数据通信系统在正常工作情况下的传输可靠性的指标，它定义为二进制数据位传输时出错的概率。

设传输的二进制数据总数为 N 位，其中出错的位数为 N_e，则误码率 P_e 表示为

$$P_e = N_e / N$$

计算机网络中，一般要求误码率低于 10^{-6}，即平均每传输 10^6 位数据仅允许错一位。如果误码率达不到这个指标，可以通过差错控制方法进行检错和纠错。

根据测试，目前电话线路在 300～2400b/s 传输速率时的平均误码率为 10^{-4}～10^{-6}；在 4800～9600b/s 传输速率时的平均误码率为 10^{-2}～10^{-4}。而计算机通信系统中对误码率的要求是 10^{-6}～10^{-9}，即平均每传送 1Mb 可能产生一位错误。

2. 信号抖动

信号抖动(signal jitter)是指数字信号在短期内重要的瞬时变化相对于理想位置发生的偏移，它与传输系统特性、信道质量及噪声等有关。

4.3 数据通信方式

通信方式按线路的工作模式分为单工、半双工和全双工通信，按通信线路分为两线制和四线制，按通信过程中是否同步分为同步传输和异步传输。

4.3.1 单工、半双工与全双工通信

信息在通信线路上传输是有方向的，根据信息在线路上的传输方向和特点，数据通信的线路工作模式分为单工、半双工和全双工 3 种。

1. 单工通信

在单工信道上信息只能在一个方向传送(见图 4-4(a))。发送方不能接收，接收方不能发送。信道的全部带宽都用于由发送方到接收方的数据传送。无线电广播和电视广播都是单工传送的例子。

2. 半双工通信

在半双工信道上(见图 4-4(b))，通信双方可以交替发送和接收信息，但不能同时发

送和接收。在一段时间内,信道的全部带宽用于一个方向上的信息传递。航空和航海无线电台及对讲机等都是以这种方式通信的。

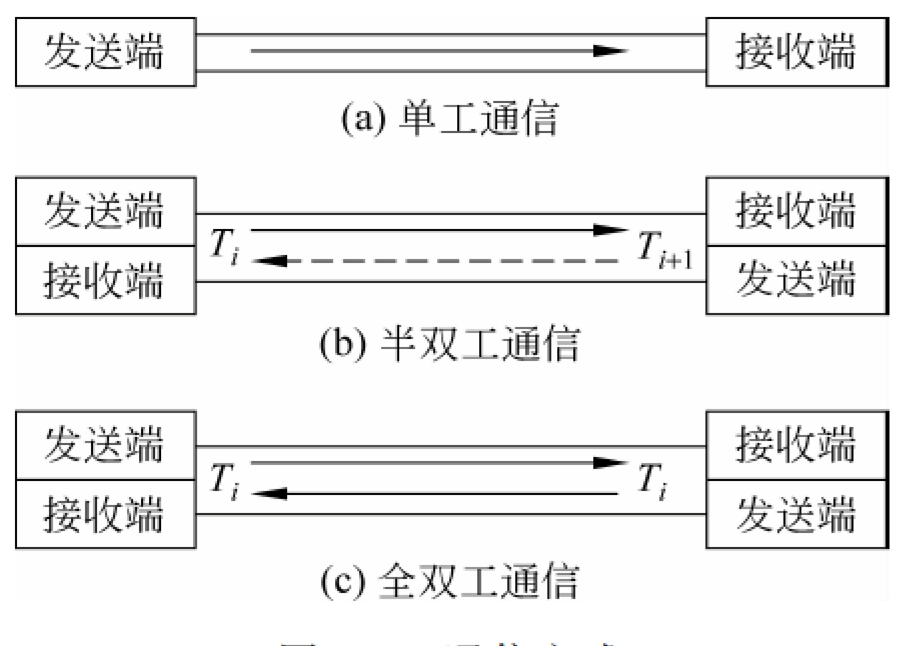


图 4-4　通信方式

3. 全双工通信

全双工通信(见图 4-4(c))是一种可同时进行信息传递的通信方式。现代的电话通信都采用这种方式。其要求通信双方都有发送和接收设备,而且要求信道能提供双向传输的双倍带宽,所以全双工通信设备较昂贵。

4.3.2　两线制和四线制

从通信线路来说,还有两线制和四线制的区别。所谓两线制,是指在两个通信调制解调器之间有两条物理连接线互相连接,两线制通常工作于半双工方式,只是在低速时可工作于全双工方式,如图 4-5 所示。

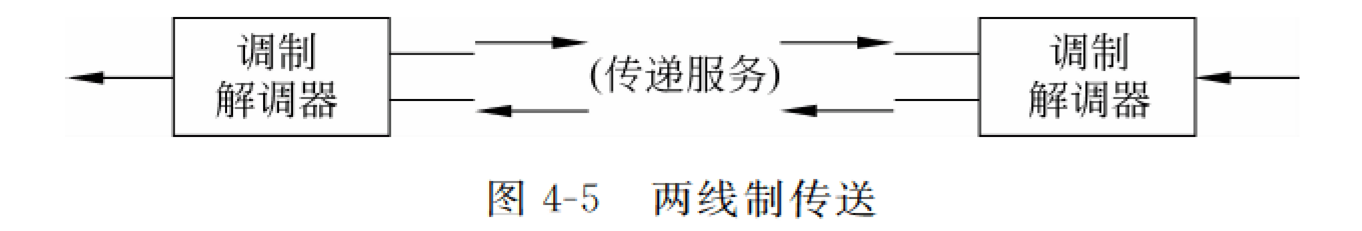


图 4-5　两线制传送

所谓四线制,是指在两个调制解调器之间有 4 条物理连接线,其中两条用于发送信号,两条用于接收信号,故可以实现全双工操作,如图 4-6 所示,现在,两线制和四线制已成为半双工和全双工的代名词了。

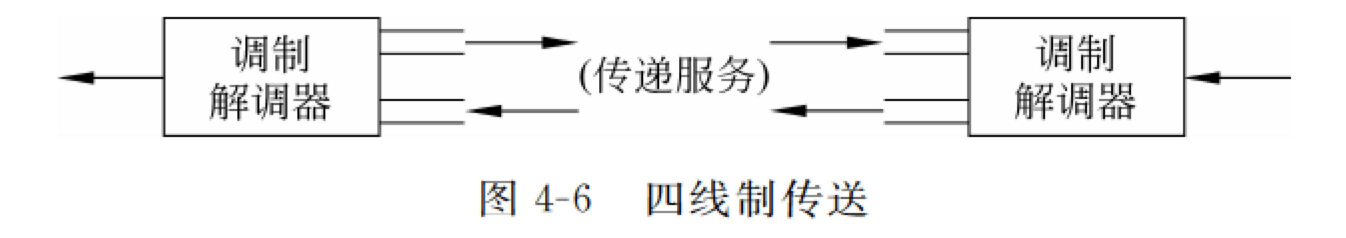


图 4-6　四线制传送

4.3.3　同步传输和异步传输

同步问题是数据通信系统中的一个重要问题。数据发送出去以后,在接收端能否被

正确地接收下来，关键就是解决同步问题。同步问题有两类：一类是位同步，指接收端需要知道每一位是什么时候开始的，从而能在一连串的位流中把每一位都分辨出来；另一类就是字符同步，即接收端需要知道什么地方是一个字符的开始位，从而能从一连串的位流中将每个字符按规定的编码格式分离出来，然后经过解码，得到需要的字符，字符同步传输也称为异步传输。

1. 异步传输

异步传输(asynchronous transmission)即把各个字符分开传输，字符与字符之间插入同步信息。这种方式也叫起止式，即在每个字符代码的前面增加一个起始位(逻辑 0)，接收端收到起始位之后，即启动一个内部位率时钟，按规则接收一个字符的代码；字符代码之后跟着一个或多个停止位(逻辑 1)。逻辑 1 有时叫做空号，而逻辑 0 有时叫做传号。用起止方式传送一个 ASCII 字符编码 R(1010010)的情况如图 4-7 所示。

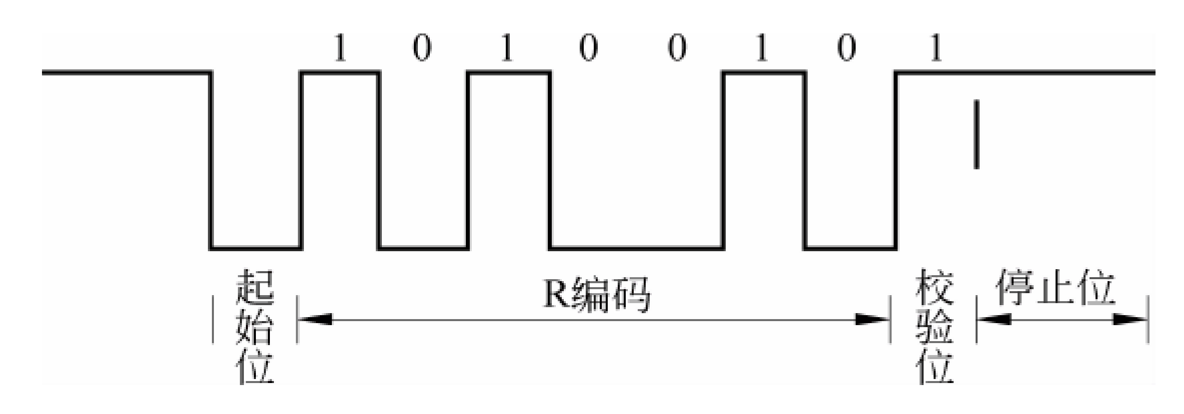


图 4-7 起止式异步传输

采用起止式异步方式，可使每个字符本身都带有所需的开始和停止的同步信息，所以在这样的系统中可以随时发送字符，使用十分方便，对于一般的电传机来说，如果字符代码占 7 位，再加上一个起始位、一个校验位和一个停止位，则发送一个字符共要占 10 个二进制位。如果传送速率为 300b/s，则相当于每秒可以传送 30 个字符。

2. 同步传输

采用同步传输(synchronous transmission)方式，发送方在发送数据之前在数据前面加上两个或两个以上的同步字符 SYN (在 ASCII 和 EBCDIC 编码表中已有定义)。在接收端，首先寻找同步字符 SYN，如果校验出两个或两个以上的 SYN，那么接下去的就全部是要求传送的字符，如图 4-8 所示。

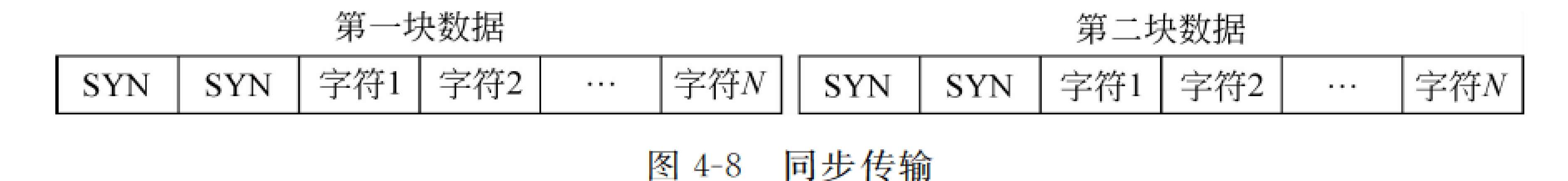


图 4-8 同步传输

采用同步方式传送，在所传送的字符与字符之间不再留有空号，也不用停顿，可以连续不停地发送，所以速度较快。

异步传输不适合传送大的数据块；而同步传输在传送连续的数据块时比异步传输更有效，因此适用于大批量的数据传送。

4.3.4 并行通信与串行通信

在数据通信中，按每次传送的数据位数，通信方式可分为并行通信和串行通信（见图 4-9）。

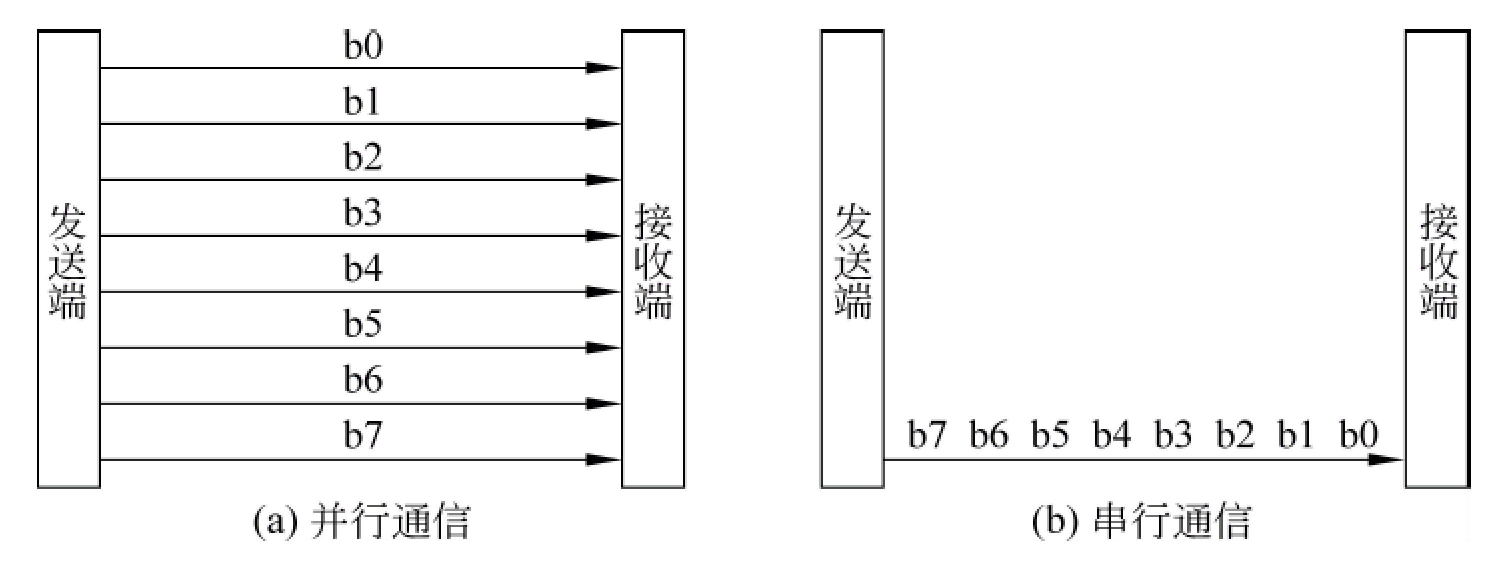


图 4-9 并/串行通信

并行通信是一次同时传送 8 位二进制数据，从发送端到接收端需要 8 根传输线。并行方式主要用于近距离通信，如在计算机内部的数据通信通常以并行方式进行。并行通信方式的优点是传输速度快，处理简单。

串行通信一次只传送一位二进制数据，从发送端到接收端只需要一根传输线。串行方式虽然传输率低，但适合于远距离传输，在公共通信系统中普遍采用串行通信方式，如公用电话系统。

4.4 数据交换方式

在通信系统中，通信过程大多是在多点之间进行的，需要利用中间节点将通信双方连接起来。因此，通信系统必须考虑所采用的数据交换方式。所谓交换技术，就是动态地分配传输线路资源的技术。常用的数据交换技术有电路交换、报文交换和分组交换等方式。

4.4.1 电路交换

电路交换要求通信双方之间建立起一条实际的物理通路，并在整个通信过程中，这条通路被通信双方独占。电话系统的信息交换方式就是典型的电路交换。在使用电话之前，必须先建立拨号连接。当拨号的信令通过许多交换机到达被叫用户所连接的交换机时，该交换机就使用户的电话机振铃。在被叫用户摘机且摘机信令传输回到主叫用户所连接的交换机后，呼叫即完成。这时，从主叫用户到被叫用户就建立了一条端到端的线路。通话完毕挂机后，挂机信令告诉这些交换机，使交换机释放刚才使用的这条线路。可见，经由电路交换而实现的通信包括以下 3 个阶段。

（1）线路建立阶段。通过呼叫完成逐个节点的接续过程，建立起一条端到端的直通线路。

（2）数据传输阶段。在端到端的直通线路上建立数据链路连接并传输数据。

（3）线路拆除阶段。数据传输完成后，拆除线路连接，释放节点和信道资源。

电路交换的优点有以下几个：通信实时性强；通路一旦建立，便不会发生冲突，数据传送可靠、迅速，不丢失且保持传输的顺序；线路传输时延小，唯一的时延是电磁信号的传播时间。其主要缺点如下：线路利用率低，特别是对于计算机的突发性数据通信不适应；通路建立之前有一段较长的呼叫建立时延；系统无数据存储及差错控制能力，不能平滑通信量。因此，电路交换适于连接时间长、批量大的实时数据传输，例如数字语音、传真等业务。对于需要经常性长期连接的用户之间，可以使用永久性连接线路或租用线路，进行固定连接，即不存在线路建立和线路拆除这两个阶段，避免了相应的时延。

4.4.2 报文交换

报文交换属存储转发交换方式，不要求通信系统为通信双方预先建立一条专用数据通路，也就不存在线路建立和线路拆除的过程。报文交换的数据传输单位是报文，传输过程采用存储-转发方式，即发送站在发送一个报文时，把目的地址附加在报文上，途经的网络节点根据报文上的目的地址信息，把报文发送到下一个节点，通过逐个节点转送直到目的站点。每个节点在收到整个报文后，暂存这个报文并检查有无错误，然后利用路由信息找出下一个节点的地址，再把整个报文传输给下一个节点。

报文交换有许多优点：不要求每条链路的数据速率相同，因而也就不必要求收、发两端工作于相同的速率；传输中的差错控制可在多条链路上进行，不必由收、发两端介入，简化了端设备；由于接力式工作，任何时刻一份报文只占用一条链路的资源，不必占用通路上的所有链路资源，而且许多报文可以分时共享一条链路，这就提高了网络资源的共享性及线路的利用率；一个报文可以同时向多个目的站发送，而电路交换网络难于做到；在电路交换网络上，当通信量变得很大时，就不能接收某些呼叫。而在报文交换网中仍可以接收报文，但是传送延迟会增加。

报文交换的主要缺点是，每一个节点对报文数据的存储转发时间较长，传输一份报文的总时间并不比采用电路交换方式短，或许会更长。因此，报文交换不适于传输实时的或交互式业务，例如，语音、传真、终端与主机之间的会话业务等。事实上，报文交换只是主要应用于非计算机数据业务（如民用电报业务）的通信网中。

4.4.3 分组交换

分组交换通常有两种方式，一种是数据报传输分组交换，简称数据报方式；另一种是虚电路传输分组交换，简称虚电路方式。

1. 数据报方式

数据报传输分组交换是国际上计算机网络普遍采用的数据交换方式。它综合报文

交换和电路交换的优点。通信系统把进网的任一分组都作为单独的“小报文”来处理，而不管它是属于哪个报文的分组，就像在报文交换方式中把一份报文进行单独处理一样。

单独处理和传输单元的“小报文”或“分组”称为数据报(data-gram)。

2. 虚电路方式

虚电路传输分组交换方式就是在发送者和接收者之间首先要建立一条逻辑电路，即建立一条虚电路，以后的数据就在虚电路中进行传输，直到通信完毕后该电路被拆除。虚电路服务方式在一条物理通路上可以建立多条逻辑通路，用户之间通信只占用其中一条逻辑通路。在分组交换方式中，由于能够以分组方式进行数据的暂时存储交换，经交换机处理后，容易实现不同速率、不同规程的终端间通信。

数据报方式和虚电路方式的主要区别在于，数据报方式没有呼叫建立过程，每个分组均带有完整的目的站地址信息，独立地选择传输路径，到达目的站的顺序与发送时的顺序可能不一致。而虚电路方式必须通过虚呼叫建立一条虚电路，每个分组不需要携带完整的地址信息，只需带上虚电路的号码标志，不需要选择路径，均沿虚电路传送，这些分组到达目的站的顺序与发送时的顺序完全一致。

4.5 信号传输复用技术

信道多路复用技术是使用带宽介质支持在同一时间、同一链路上发送多个不同信息流的数据通信技术。在同一信道上同时传输多路不同信号而互不干扰，以提高通信线路的利用率。常用的多路复用技术有频分多路复用技术(FDM)和时分多路复用技术(TDM)。

在计算机网络的信道中还广泛使用统计时分复用(STDM)、密集波分复用(DWDM)和码分多址(CDMA)技术。

4.5.1 频分多路复用

频分多路复用(Frequency Division Multiplexing，FDM)，是将具有一定带宽的信道分割为若干个有较小频带的子信道，每个子信道供一个用户使用。这样在信道中就可同时传送多个不同频率的信号，如图 4-10 所示。被分割开的子信道的中心频率不相重合，且各信道之间留有一定的空闲频带(也叫做保护频带)，以保证数据在各子信道上的可靠传输。频分多路复用实现的条件是信道的带宽远远大于每个传输单路信号所需要的带宽。

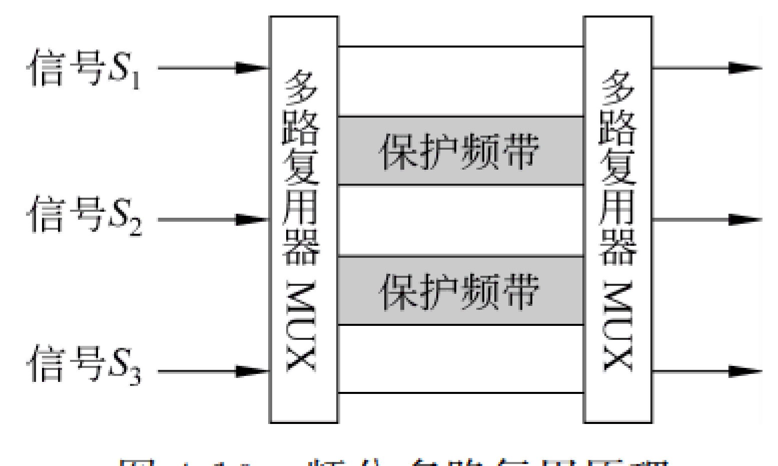


图 4-10　频分多路复用原理

4.5.2 时分多路复用

1. 时分多路复用原理

时分多路复用(Time Division Multiplexing,TDM),是将一条物理线路按时间分成一个个的时间片,每个时间片常称为一帧(frame),再分为若干时隙,轮换地为多个信号所使用。每个时隙由一个信号(即一个用户)占用,即在占有的时隙内,该信号使用通信线路的全部带宽,而不像 FDM 那样,同一时间同时发送多路信号,如图 4-11 所示。时隙的大小可以按一次传送一位、一个字节或一个固定大小的数据块所需的时间来确定。从性质上来说,时分多路复用特别适合于数字信号的场合。

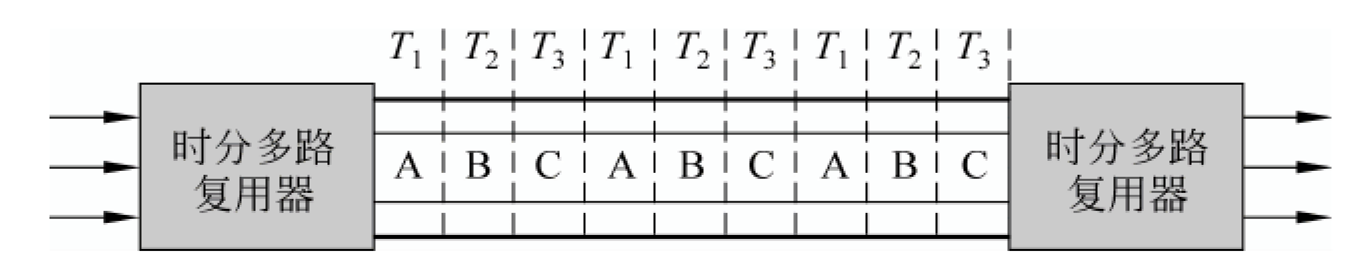


图 4-11　时分多路复用原理

通过时分多路复用,多路低速数字信号可复用两条高速的信道。例如,数据速率为 48kbps 的信道可为 5 条 9600bps 速率的信号时分多路复用,也可为 20 条速率为 2400bps 的信号时分多路复用。

表 4-1 对频分多路复用和时分多路复用进行比较。

表 4-1　频分多路复用和时分多路复用的比较

分　类	特点(共享信道方式)	优　点	缺　点
频分多路复用	同一时间传送多路信号,采用带宽划分方法	适用于传输模拟信号,无延时,费用低	速率低
时分多路复用	多个信号分时使用一个信道,采用时间片轮转方法	速率高,适用于传输数字信号,传输效率高	有一定的延时,费用较高

2. 同步时分多路复用和异步时分多路复用

同步时分多路复用是指时分方案中的时间片是预先分配好的,时间片与数据源是一一对应的,不管某一个数据源有无数据要发送,对应的时间片都是属于它的,或者说各数据的传输定时是同步的。在接收端,根据时间片的序号来分辨是哪一路数据,以确定各时间片上的数据应当送往哪一台主机。

异步时分多路复用是指各时间片与数据源无对应关系,系统可以按照需要动态地为各路信号分配时间片,各时间片与数据源无对应关系。为使数据传输顺利进行,所传送的数据中需要携带供接收端辨认的地址信息,因此异步时分复用也称为标记时分复用技术。

4.5.3 波分复用技术

波分复用技术是指在同一根光纤上同时传送多个波长不同的光载波，光载波间隔仅0.8nm或1.6nm。第二代密集波分复用系统(DWDM)已做到在一根光纤上复用80～160个光载波信号，每个波道的数据传输速率高达10Mbps。在工程上，一根光缆中可捆扎100根以上的光纤，得到的总数据传输速率达4Tbps。波分复用(WDM)用于光缆传输的网络，不同的信号被携载在光的不同波长上。光载波信号被数字信号调幅传输一段距离后就会衰减，一般用光纤放大器(EDFA)放大，两个光纤放大器之间的线路长度可达120km。

波分复用的原理如图4-12所示，在发送端将不同波长的光信号组合起来，复用到一根光纤上，在接收端又将组合的光信号分解，并送入不同的终端。

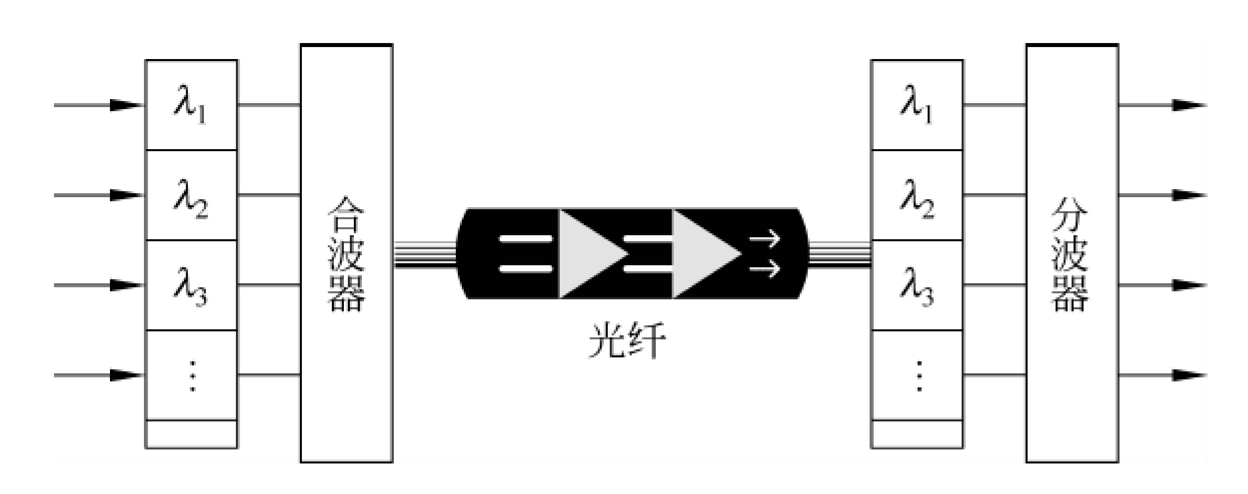


图4-12 波分复用原理

4.5.4 码分多址技术

码分多址技术广泛用于民用的移动通信，特别是无线局域网中。其基本原理是将每一个比特时间再划分为 m 个间隔（称为码片），码分多址技术为一个站分配一个唯一的 m 位码片序列，指定信息0和1的 m 位二进制码（互为反码）。如8位码片系列分配给S站的码片系列为0～11100100，1～00011011。码分多址技术可提高通信的语音质量和数据传输的可靠性，增大通信系统的容量，降低手机的平均发射功率，目前已广泛用于无线通信中。

4.6 信号传输差错控制

数字信号传输中，由于信道不理想以及加性噪声的影响，被传输的信号码元波形会变坏，造成接收端错误判定。为了尽量减小数字通信中信息码元的差错概率，应及时地自动检验差错，并进一步做到自动校正，这就是数字通信系统中重要的差错控制技术。通常，差错控制的解决方法是采用抗干扰编码或纠错编码。

4.6.1 检错码与纠错码

在传输过程中发生错误后，接收端自动检查并发现错误的编码技术称为检错码。检错码通常是指发送端在发送每一组信息时发送一些附加位，接收端对这些附加位数据进行判断，看其是否正确，如果存在错误，把错误的结果回馈给发送端，让发送端重新发送该信息，直至接收端收到正确的数据为止。

纠错码是在传输过程中发生错误后能在接收端自行发现或纠正的信道编码。为了使一种码具有检错或纠错能力，必须对原码字增加多余的码元，以扩大码字之间的差别，使一个码字在一定数目内的码元上发生错误时不致错成另一个码字。接收端收到码字后，用编码时所用的规则去检验，根据编码规则是否满足以判定有无错误。当不能满足编码规则时，在可纠能力之内按一定的规则确定错误所在的位置，并予以纠正。现在比较常见的纠错码有海明纠错码和正反纠错码等。下面介绍几种简单的校验技术。

4.6.2 奇偶校验

奇偶校验又叫字符校验，或叫垂直冗余校验(Vertical Redundancy Code，VRC)，是一种简单的校验方法。奇偶校验是在传输信息位的后面另外增加一个二进制位，该位叫做校验位，其主要目的是使传输信息编码中的 1 或 0 的个数成为奇数或偶数。如果使编码中 1 的个数成为奇数则叫做奇校验，反之则叫做偶校验。

例如，传输字符 R 的 ASCII 码为 1010010，进行奇校验时后面增加一位 0，即传输 10100100，1 的个数为奇数；进行偶校验时后面增加一位 1，即传输 10100101，1 的个数为偶数。

奇偶校验能够检测出信息传输过程中的部分误码，其中 1 位误码能检出，2 位及 2 位以上误码不能检出；另外，它不能纠错。在发现错误后，只能要求重发。但由于其简单实用，仍得到了广泛使用，多用于低速、近距离、低成本通信。

4.6.3 方块校验

方块校验又叫报文校验或纵向(水平)冗余校验(Level Redundancy Code，LRC)，这种方法是在垂直校验的基础上，在一批字符传送之后，另外再增加一个检验字符，该字符的编码方法是使每一位纵向代码中 1 的个数成为奇数 (或偶数)，如表 4-2 所示。

采用这种校验之后，如果其中有一个二进制位出错，不仅从一行中的 VRC 校验位中能反映出来，同时从一个纵列的 LRC 校验位中也能反映出来，根据垂直和水平两个校验位的反映，可以确定出错的位置，从而加以校正。采用这种办法之后，不仅可以检验出 1 位出错，而且可以自动纠正 1 位差错，使误码率能降低，纠错效果十分显著。

表 4-2 方块校验举例

字　符	二进制码	字　母	奇偶校验位(奇)
字符 1	1000010	B	1
字符 2	1000001	A	1
字符 3	1010011	S	1
字符 4	1001001	I	0
字符 5	1000011	C	0
字符 6	1010010	R	0
方块校验符(奇)	1110111	w	0

4.6.4 循环冗余校验

循环冗余校验(Circular Redundancy Code,CRC)是通信系统与磁介质记录中通常采用的编码校验技术,在网络数据通信中也有较好的差错校验效果。

循环冗余校验工作方式是:在发送端,将传输信息的 K 位二进制码组之后加入 R 位校验码(即冗余位),使整个编码长度变为 N 位,进行发送。在接收端,根据通信双方约定的生成多项式 $G(x)$进行检验,以确定传送中是否出错。这种编码也称为(N,K)码。

在代数编码理论中,对于一个给定的(N,K)码,可以证明存在一个最高次幂为 $N-K=R$ 的多项式 $G(x)$,它可以生成 R 位信息的校验码(CRC)。

如何确定二进制码组的多项式呢?实际应用中是将一个码组表示为一个多项式,码组中各码位作为多项式的系数。

例如,二进制码组 1100101,转换为多项式为

$$1 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1$$

则该码组对应的多项式为

$$x^6 + x^5 + x^2 + 1$$

下面介绍循环冗余校验编码方式。设编码前的原始 K 位信息多项式为 $P(x)$,则 $P(x)$的最高幂次加 1 等于 K;设生成多项式为 $G(x)$,其最高幂次等于 R,则 CRC 多项式为 $R(x)$;编码后带 CRC 的 N 位信息多项式为 $T(x)$。

编码信息表达式如下:

$$T(x) = X^R P(x) + R(x)$$

$$R(x) = X^R P(x) / G(x) \text{(模 2 除)}$$

其中:

$X^R P(x)$是原始 K 位信息码序左移 R 位。

$R(x)$是冗余信息位。

$G(x)$是生成多项式。

例如,设信息码为 1100,生成多项式码为 1011。则有

$$P(x)=x^3+x^2,\quad G(x)=x^3+x+1,\quad R=3$$
$$X^R P(x)=x^3(x^3+x^2)=x^6+x^5$$

上式表示二进制码序列为 1100000，即 $P(x)$二进制码序左移 3 位。

$X^R P(x)/G(x)$得余式

$$R(x)=x$$

即二进制码序列为 010。则

$$T(x)=X^R P(x)+R(x)=x^3(x^3+x^2)+x=x^6+x^5+x$$

因此，发送端 $T(x)$二进制码序列为

$$1100000+010=1100010$$

对于接收端来说，接收到 $T(x)$后，除以 $G(x)$，若余式为 0 传输正确，反之错误。

4.7　本章小结

数据通信的目地是交换信息。信息的载体可以是多媒体，包含语音、音乐、图形图像、文字和数据等。为了传送这些信息，首先要进行二进制编码处理，这些被传输的二进制代码称为数据。在数据通信系统中，传输模拟信号的系统称为模拟通信系统，而传输数字信号的系统称为数字通信系统。数据通信系统的基本通信模型是：产生和发送信息的一端叫信源，接收信息的一端叫信宿，信源与信宿通过信道进行通信。数据通信的线路工作模式分为单工、半双工和全双工 3 种。

信道多路复用技术是使用带宽介质支持在同一时间、同一链路上发送多个不同信息流的数据通信技术。信号传输的复用技术包括频分多路复用技术、时分多路复用技术、波分多路复用技术及码分多址技术等。

信号传输过程中由于种种原因会出现差错，常见的差错校验方法有奇偶校验和循环冗余校验等。

综合训练

一、理论题

1. 选择题

(1) 数字信号传输速率在数值上等于每秒钟传输的二进制比特数，单位为(　　)。

A. 码元　　B. 比特　　C. 比特/秒　　D. 波特

(2) 在数据通信系统中，传输数字信号的系统称为(　　)系统。

A. 数字通信　　B. 模拟通信　　C. 数据通信　　D. 网络通信

(3) 半双工数据传输是(　　)。

A. 双向同时传输　　B. 双向不同时传输

C. 单向传输　　D. A 和 B 都可以

(4)在数据传输过程中,为发现误码甚至纠正误码,通常在原数据上附加校验码,其中功能较强的是(　　)。

A. 奇偶校验码　　B. 循环冗余码　　C. 交叉校验码　　D. 横向校验码

(5) 将家用 ADSL 接入网络,其信道复用技术称为(　　)。

A. 时分多路复用技术　　B. 码分多址技术

C. 波分多路复用技术　　D. 频分多路复用技术

2. 填空题

(1) 在计算机科学中,数据是指________并被计算机程序处理的________的总称。

(2) 信号是运载消息的工具,可分为________和________信号。

(3) 通信系统三要素是________、________和________。

(4) 半双工数据传输是通信双方可以在________方向上进行数据传输,但不能同时________。

(5) 按传输过程中是否同步可将数据传输分为________和________。

(6) 信息交换方式有________、________和________。

(7) 多路复用的理论依据是________在频分多路复用的各子频带间留有一定的保护频带,其目的是________。

(8) 通常在纠、检错编码中引入的监督码元越多,________越强。

3. 简述题

(1) 简述信息、数据和信号这 3 个概念之间的关系。

(2) 通信系统的基本模型是什么?

(3) 数字信号如何在模拟信道上传输?

(4) 什么叫做同步? 为什么需要同步这种技术?

(5) 数据交换有几种方式? 各有哪些优缺点?

二、实践题

1. 求解

(1) 设信道带宽为 4kHz,信噪比为 30dB,根据香农公式,求该有噪信道的最大限制数据速率。

(2) 参考表 4-2,编写"Administration"一词的方块奇校验。

2. 常用网络命令的使用

(1) ping 命令是测试网络连接及信息包发送和接收状况非常有用的工具,是网络测试最常用的命令,如图 4-13 所示。

命令格式:

```
ping [IP 地址或域名] [-t] [-a] [-n count] [-l size] [/?]
```

/?：帮助信息，显示命令的语法格式及参数说明。

-t：不间断地向目标 IP 发送数据包，直到用户强制其停止为止。

-l：定义发送数据包的大小，默认为 32B，最大为 65 500B。

-a：解析已知 IP 地址的目标主机的计算机名称。

-n：定义向目标 IP 发送数据包的次数，具体次数由 count 来指定，默认为 3 或 4 次。

```
管理员: C:\Windows\system32\cmd.exe - ping  -t 192.168.1.1
C:\Users\Administrator>ping -t 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=255
```

图 4-13　ping 命令

（2）ipconfig 命令以窗口形式显示本机中 IP 协议的配置信息，包括网络适配器的物理地址、主机的 IP 地址、子网掩码以及默认网关等，如图 4-14 所示。



图 4-14　ipconfig 命令

命令格式：

```
ipconfig [/all] [/release] [/renew] [/?]
```

/?：帮助信息，显示命令的语法格式及参数说明。

/all：显示本机全部的网络配置信息。

/release：释放指定网卡的 IP 地址。

/renew：为指定网卡重新分配 IP 地址。

(3) net 命令是网络命令中最重要的一个命令，是多个子命令的集合。

命令格式：

```
net [/?] [net 子命令]
```

/?：帮助信息，显示命令的语法格式及参数说明。

最常用的 net 子命令如下：

view：用于查看远程主机的所有共享资源。

use：把远程主机的某个共享资源映射为本地盘符以方便使用。

start/stop：用于查看、启动、停止主机上的某个服务。

user：用来查看和管理与账户有关的事务，包括新建账户、删除账户、查看特定账户、激活账户及禁用账户等。

例如，将远程主机的某个共享资源映射为本地盘符：

```
net use<驱动器盘符：>\\IP 地址\共享名    (共享资源映射)
net use<驱动器盘符：>/delete            (断开网络映射)
```

(4) tracert 命令用来显示数据包到达目标主机所经过的路径以及到达每个节点的时间，即路由跟踪。

命令格式：

```
tracert [/?] [参数]
```

/?：帮助信息，显示命令的语法格式及参数说明。

常用参数如下：

-d：不解析目标主机名字。

-h maxnum：指定搜索到目标地址的最大跳数。

-w timeout：指定超时时间间隔，时间单位为 ms。

例如，查看本地主机与指定域名的目标主机之间的传输情况：

```
Tracert www.sunline.com
```

(5) netstat 命令用来帮助网络管理员了解网络的整体使用情况，包括当前正在工作的网络连接的详细信息，例如网络连接、路由表和网络接口信息，从而可以统计目前共有哪些网络连接正在运行，如图 4-15 所示。

命令格式：

```
netstat [/?] [参数]
```

/?：帮助信息，显示命令的语法格式及参数说明。

常用参数如下：

-a：显示所有活动的 TCP 连接及计算机侦听的 TCP 和 UDP 端口。

-e：显示以太网统计信息，如发送和接收的字节数及数据包数。

-s：按协议显示统计信息。

-r：显示 IP 路由表的内容。

例如，显示所有活动的 TCP 连接及计算机侦听的 TCP 和 UDP 端口：

```
Netstat -a
```

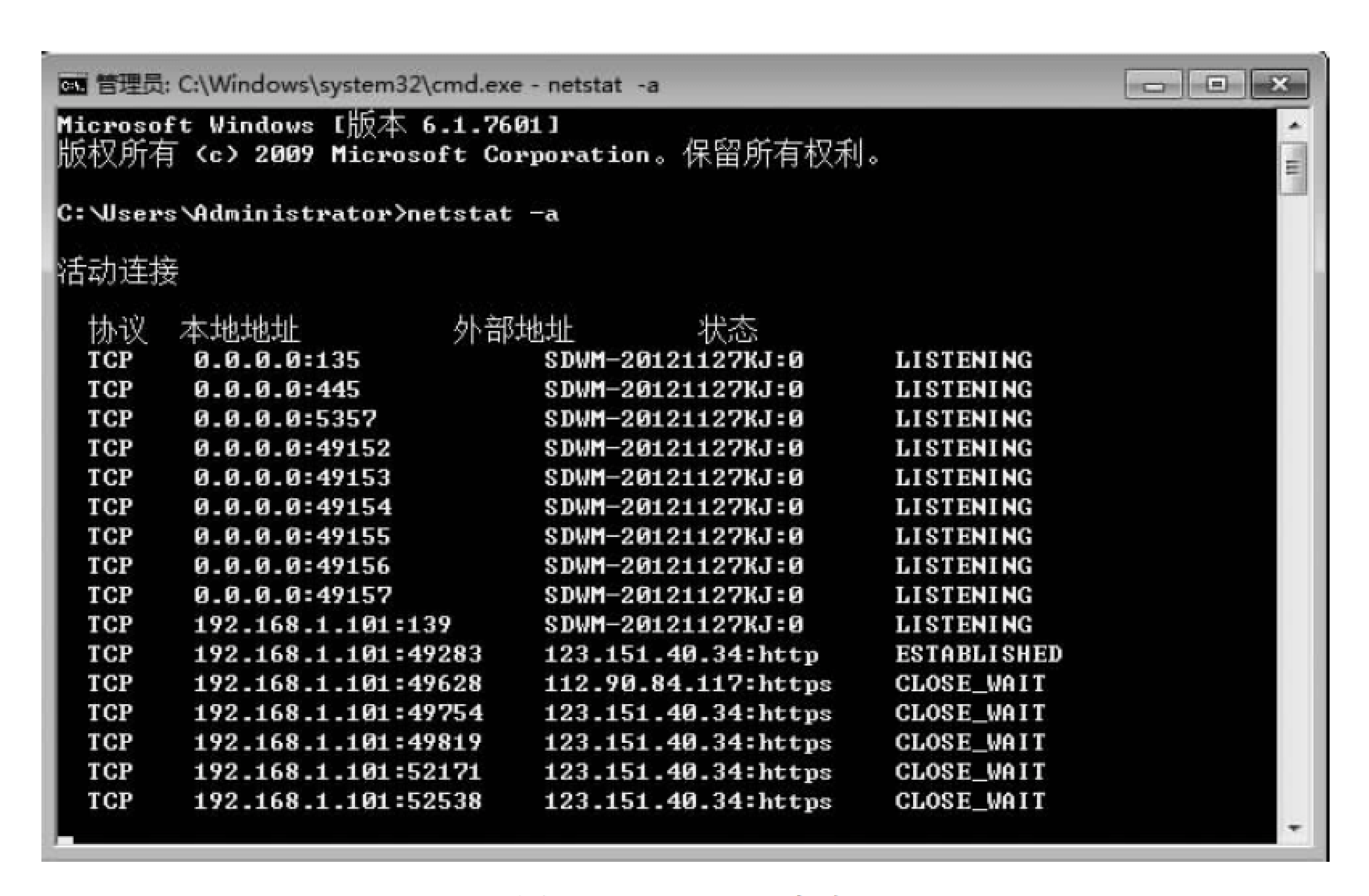


图 4-15 netstat 命令

第 5 章　通信介质及主要特征

本章主要内容

- 同轴电缆及其应用
- 双绞线及其应用
- 光纤及其应用
- 无线通信介质简介

通信介质也称通信传输介质，一般简称传输介质，是指通信双方建立通信线路、传送信息的载体。常用的传输介质分为有线传输介质和无线传输介质两大类。

有线传输介质是指在两个通信设备之间实现的物理连接部分，它能将信号从一方传输到另一方，有线传输介质主要有双绞线、同轴电缆和光纤。双绞线和同轴电缆传输电信号，光纤传输光信号。

无线传输介质指我们周围的自由空间。利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可分为无线电波、微波、红外线和激光等，信息被加载在电磁波上进行传输。

5.1　同轴电缆及其应用

在 20 世纪 80 年代，同轴电缆是非常流行的一种传输介质，它有以下几个优点：是以太网的基础；适用于相对长的无中继器的线路上；支持高带宽通信；抗干扰性强。

5.1.1　物理特性

同轴电缆(coaxial cable)是一种电线及信号传输线，一般由 4 层物料制成：最里面是一条导电铜芯，芯线的外面有一层塑胶绝缘体，构成内绝缘体屏蔽层，内绝缘体外面又有一层薄的网状导电体(一般为铜或合金)，最外层的绝缘物料作为外皮，其结构如图 5-1 所示。

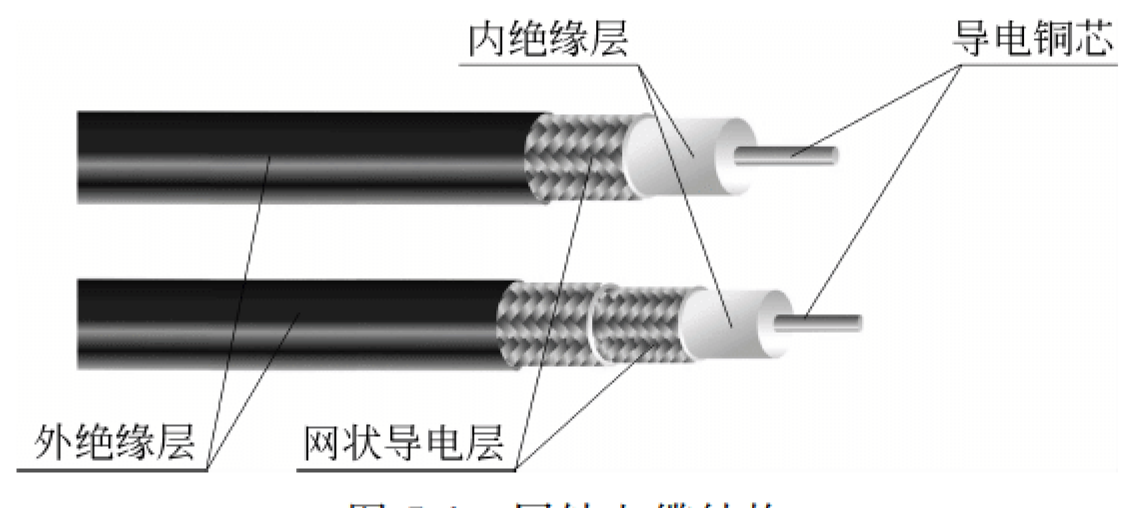


图 5-1　同轴电缆结构

5.1.2 传输特性

同轴电缆从用途上分可分为基带同轴电缆和宽带同轴电缆。

基带同轴电缆：特性阻抗为50Ω，特点是阻抗均匀，具有高带宽和极好的噪声抑制特性，误码率较低，数字信号可直接加载到电缆上，适用于各种局域网络。基带同轴电缆按其直径分为粗同轴电缆与细同轴电缆。粗缆适用于比较大型的局部网络，它的标准距离长、可靠性高。由于安装时不需要切断电缆，因此可以根据需要灵活调整计算机的入网位置。但粗缆网络必须安装收发器和收发器电缆，安装难度大，所以总体造价高。相反，细缆安装则比较简单，造价低，但安装过程要切断电缆，两头须装上基本网络连接头(BNC)，然后接在T型连接器两端。

宽带同轴电缆是特性阻抗为75Ω的CATV电缆。在计算机网络中，任何使用模拟信号进行传输的电缆统称为宽带电缆，在标准有线电视技术的支持下，可使用的频带高达300MHz(常常达到450MHz)，尽管其传输性能要高于基带同轴电缆，但它需要模拟放大器周期性地加强信号，而这些放大器又仅能单向传输信号，因此增加了宽带同轴电缆的安装难度。目前宽带同轴电缆应用于长途电话网、电缆电视系统和宽带计算机网络。基带同轴电缆和宽带同轴电缆的特征对照见表5-1。

表5-1 基带同轴电缆和宽带同轴电缆的特征对照

同轴电缆		特性阻抗/Ω	直径/cm	传输距离/m	特点
基带同轴电缆	粗同轴电缆	50	1.27	500	用于数字传输
	细同轴电缆	50	0.26	180	用于数字传输
宽带同轴电缆		75			用于模拟传输

5.1.3 连通性

同轴电缆可以用于点对点的连接，也可以用于多点的连接。其中，基带同轴电缆支持数百台设备的连接，而宽带同轴电缆则可支持数千台设备的连接，但这也暴露出了一个问题，当接头多时容易产生隐患，无论是基带同轴电缆还是宽带同轴电缆均为总线型拓扑结构，即一根缆上接多部计算机，尽管这种拓扑结构适用于计算机密集的环境，但是当某一触点发生故障时，故障会串联影响到整根缆上的所有计算机。故障的诊断和修复都很麻烦。另外，它在与计算机网卡相连时还需要T型连接器(如图5-2所示)，因此，同轴电缆已逐步被非屏蔽双绞线或光缆取代。



图5-2 T型连接器

5.1.4 地理范围

基带同轴电缆使用的最大距离限制在几公里以内，而宽带同轴电缆则可以达到几十公里。

5.1.5 抗噪性和经济性

因为同轴电缆中具有绝缘体和屏蔽层，所以它的抗噪性介于双绞线和光缆之间。另外，由于制作工艺较为复杂和材料成本的原因，同轴电缆价格介于双绞线和光缆之间。同轴电缆的使用和后期维护也比较方便。

5.2 双绞线及其应用

双绞线(twisted pair)是由两条相互绝缘的导线按照一定的规格互相缠绕在一起而制成的一种通用配线，属于信息通信网络传输介质。

双绞线过去主要是用来传输模拟信号的，但现在同样适用于数字信号的传输。

5.2.1 物理特性

把两根绝缘的铜导线按一定规格互相绞在一起(如图5-3所示)，可降低信号干扰的程度，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。其中外皮所包的导线两两相绞，形成双绞线对，因而得名双绞线。通常双绞线有4个绞对，共8芯。双绞线的连接器为RJ-45，俗称水晶头。

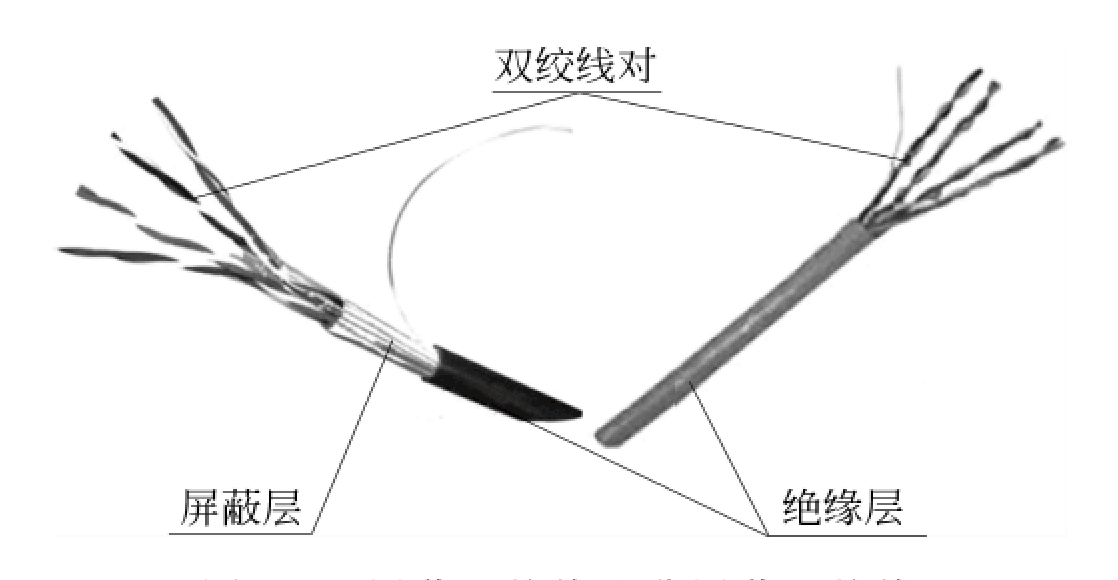


图5-3 屏蔽双绞线和非屏蔽双绞线

在双绞线电缆内，不同线对具有不同的扭绞长度，一般地说，扭绞长度在3.81～14cm内，按逆时针方向扭绞。相邻线对的扭绞长度在1.27cm以上，一般绞线扭绞(或称缠绕)越密，其抗干扰能力就越强。需要注意的是，由于双绞线的应用领域和应用目的的不同，出现了数百种不同的设计形式。这些设计的主要区别点在于它们的缠绕率、导线对的数目、铜线级别以及是否具有屏蔽能力等。

双绞线是目前局域网中最为常见的通信媒介。局域网中所采用的双绞线可以分为两类：

(1) 屏蔽双绞线(STP)。

(2) 非屏蔽双绞线(UTP)。

屏蔽双绞线与非屏蔽双绞线的区别在于是否有金属制成的屏蔽层。

5.2.2 传输特性

在局域网中常用的双绞线根据其传输特性可以分为 7 类，见表 5-2。在典型的以太网中，常用三类(CAT-3)、五类(CAT-5)及超五类(CAT-5e)非屏蔽双绞线。目前，超五类(CAT-5e)非屏蔽双绞线应用比较普遍。

表 5-2 七类非屏蔽双绞线传输特性对照表

双绞线型号	行业标准界定	最大传输频率/MHz	最大传输速率	应用范围
CAT-1	未被 EIA/TIA 承认			电话网络、ISDN 线路
CAT-2	未被 EIA/TIA 承认	1	4Mbps	4Mbps 的令牌环网络
CAT-3	被 ANSI 和 EIA/TIA568 所界定及承认	16	10Mbps	10Mbps 以太网络
CAT-4	未被 EIA/TIA 承认	20	16Mbps	16Mbps 的令牌环网络
CAT-5	被 EIA/TIA-568-B 所界定及承认	100	100Mbps	快速以太网(100Mbps)
CAT-5e	被 EIA/TIA-568-B 所界定及承认	100	1Gbps	快速以太网(1Gbps)
CAT-6	被 EIA/TIA-568-B 所界定及承认	500	10Gbps	快速以太网(1.5Gbps)
CAT-6a	未被 EIA/TIA 承认	500	10Gbps	万兆以太网(10Gbps)
CAT-7	ISO/IEC 11801 Class F 缆线标准的非正式名称	600	10Gbps	

5.2.3 连通性

双绞线既可以点对点的连接，也可以用于多点的连接，这些性质与同轴电缆相同。

5.2.4 地理范围

双绞线用于远程中继线时，最大的距离可以达到 15km，而在 10～100Mbps 的局域网中，每个网段的最大长度是 100m。它们的跨度小于同轴电缆所提供的跨度，这主要是因为双绞线的抗干扰能力小于同轴电缆，更容易受到环境噪声的影响。

5.2.5 抗噪性

各种不同的双绞线抗噪性区别很大，主要取决于扭绞程度和适当的屏蔽。在一对导线中，每厘米的扭绞越多，所对应的抗噪性就越优秀。

5.2.6 经济性及选购

双绞线的价格远低于其他的传输介质，且易于安装和维护，是较为理想的传输介质。

在双绞线选购时，符合质量标准的双绞线具有以下3方面特点：

(1) 双绞线的绝缘胶皮要耐高温、不易燃。

(2) 双绞线要具有一定的抗拉伸性。

(3) 双绞线要既容易弯曲，又不易折断。

5.3 光纤及其应用

5.3.1 物理特性

光纤(optical fiber)是光导纤维的简写，是一种利用光在玻璃或塑料制成的纤维中的全反射原理而制成的光传导工具。通常光纤的直径为50～100μm，柔软，能传导光波。按照光纤的材料，可以将光纤的种类分为石英光纤和全塑光纤。光纤的结构如图5-4所示。

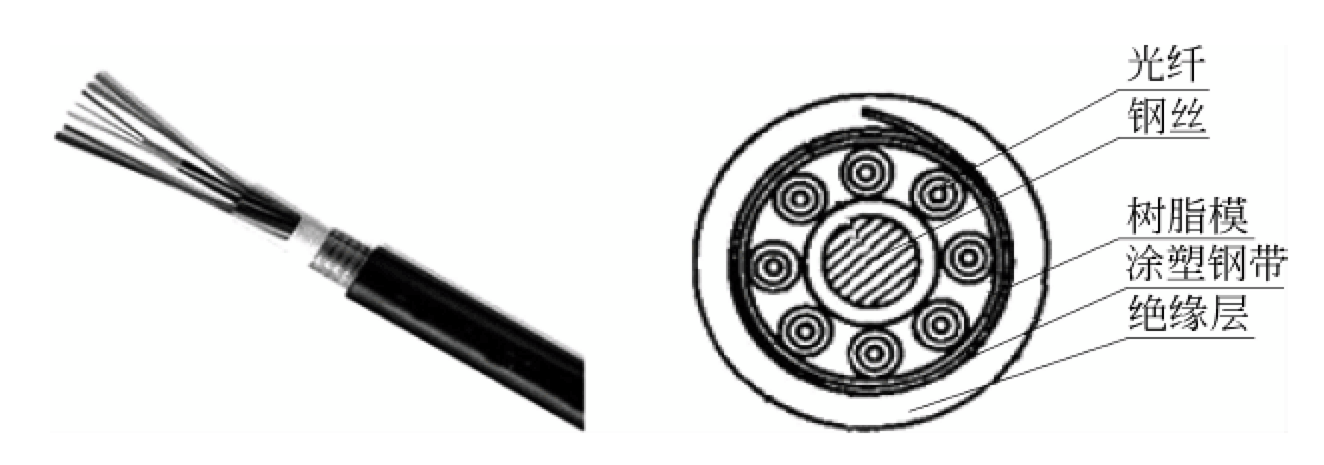


图5-4 光纤结构

石英光纤一般是指由掺杂石英芯和掺杂石英包层组成的光纤。这种光纤有很低的损耗和中等程度的色散。目前通信用光纤绝大多数是石英光纤。

光纤与同轴电缆的结构非常相似，只不过光纤没有电缆那一层密织的网用来屏蔽，因为光纤本身就具有非常高的屏蔽性能，无须另外的屏蔽层。光纤的分类标准很多，主要可以从工作波长、折射率分布、传输模式、原材料和制造方法等方面来进行分类。下面主要介绍传输模式与纤芯直径分类。

1. 传输模式分类

光纤按传输模式可分为单模光纤和多模光纤两类。单模光纤只传输一种模式，纤芯

直径较细，通常在 8～10μm 范围内。而多模光纤可传输多种模式，纤芯直径较粗，典型尺寸为 50μm 左右，相当于一根头发丝那么精细。

1）单模光纤（Single-Mode Fiber，SMF）

单模光纤只传输主模，也就是说光线只沿光纤的内芯进行传输。单模光纤携带单个频率的光将数据从光纤的一端传输到另一端，如图 5-5(a)所示。

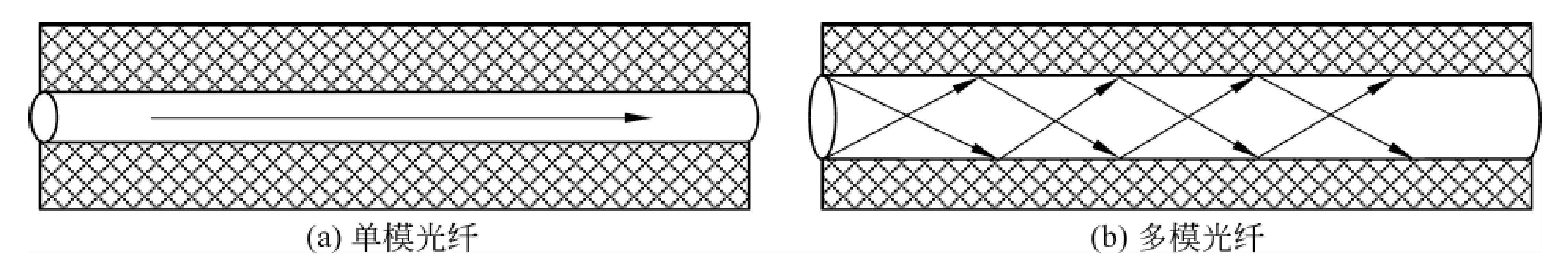


图 5-5 单模光纤、多模光纤信号传输示意图

SMF 光纤直径较细，约为 10μm。单模光纤使用的光波长为 1.31μm 或 1.55μm。目前在有线电视和光通信中，SMF 光纤是应用最广的一种光纤。

2）多模光纤（Multi-Mode Fiber，MMF）

多模光纤可以在单根或多根光纤上同时携带几种光波，如图 5-5(b)所示。

MMF 光纤纤芯直径较粗，通常为 50μm 或 62.5μm。由于其模间色散较大，限制了传输数字信号的频率，而且这一问题随距离的增加会更加严重。例如，600Mbps/km 的光纤在 2km 时则只有 300Mbps 的带宽了。因此，多模光纤传输的距离比较近，一般只有几千米。

2. 纤芯直径分类

如果按纤芯直径大小来分，可以将光纤分为以下类型。

（1）缓变型多模光纤：50/125μm。

（2）缓变增强型多模光纤：62.5/125μm。

（3）突变型单模光纤：8.3/125μm。

5.3.2 传输特性

多条光纤组织成一束，就构成了一条光缆。光缆是通过内部的全反射来传输一束经过编码的光信号。由于光纤的折射率高于外部包层的折射率，因此，可以形成光波在光纤与包层的界面上的全反射。

典型的光纤传输系统的结构如图 5-6 所示。在发送端，主要采用两种光源：发光二极管(LED)与注入型激光(ILD)。在接收端将光信号转换成电信号时，要使用光电二极

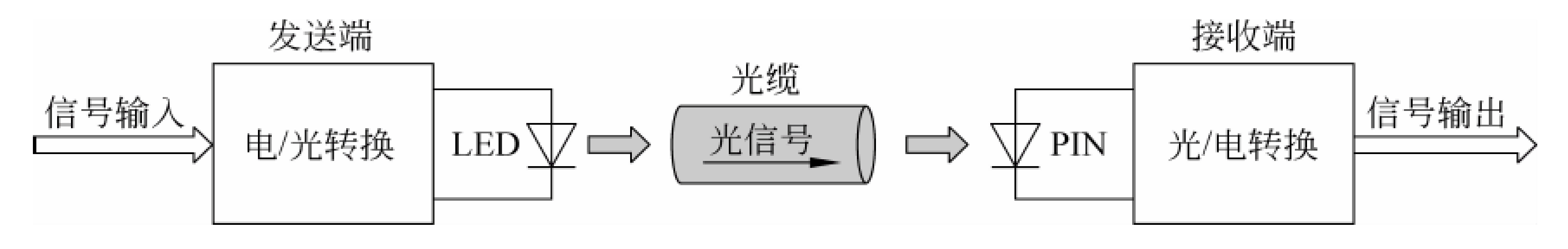


图 5-6 光纤传输结构

管 PIN 检波器或 APD 检波器。光载波调整方法采用振幅键控(ASK)调制方法,即亮度调制。因此,光纤传输速率可以达到几千 Mbps。

5.3.3 连通性

在网络数据通信中,应用光缆进行数据传输通常采用点对点连接方式。不过,在某些实验系统中,也可以采用多点连接的方式。

5.3.4 地理范围

由于光纤数据传输时损耗极低,所以在不使用中继器的情况下,可以在 6～8kM 的范围内进行高速传输数据。

5.3.5 抗噪性和经济性

因为光纤的基本成分是石英,只传光,不导电,不受电磁场的作用,在其中传输的光信号不受电磁场的影响,故光纤传输对电磁干扰和工业干扰有很强的抵御能力。也正因为如此,在光纤中传输的信号不易被窃听,因而利于保密。又因为光纤传输一般不需要中继放大,不会因为放大引入新的非线性失真。只要激光器的线性好,就可高保真地传输电视信号。

综合来看,用光纤来传递数据时,在抗噪性能上是无与伦比的。

光纤相较于铜导线具有以下优点:

(1) 光纤能提供比铜导线高得多的带宽,传输速率极高。

(2) 光传输时衰减小,可传输距离更远。

(3) 光纤无串音干扰,数据不易被窃听和截取,因而安全保密性好。

(4) 光纤不受电磁干扰,不受空气中腐蚀性物质的侵袭,可以在恶劣环境下工作。

尽管目前来看光纤的单价还较高,但是从长远来看,随着制造的成本不断下降以及光纤传输所占据的绝对优势,光纤必将普及应用。

5.4 无线传输介质简介

在自由空间利用电磁波发送和接收信号进行通信称为无线传输。地球上的大气层为大部分无线传输提供了物理通道,就是常说的无线传输介质。无线传输所使用的频段很广,人类现在已经利用了许多个波段进行通信。无线通信的方法有无线电短波、微波、红外线、激光以及卫星通信等。

在电磁波信息传输中,光波占有很重要的地位。

5.4.1 无线电波

无线电波是指在自由空间(包括空气和真空)传播的射频频段的电磁波,按波长划分包括长波、中波、短波以及微波等。

无线通信的基本原理是通过电磁转换实现通信。通过调制将信息加载于无线电波之上,当电波通过空间传播到达接收端,电波引起电磁场变化,通过解调将信息提取出来,就达到了信息传递的目的。

无线通信的基本特点如下:

(1) 采用无线信道,可同时向多个接收端传送信号。

(2) 不受自然条件限制,广泛适用于各种地形。

(3) 适合宽带通信,可应用于移动通信。

(4) 电波容易受到干扰,保密性差。

(5) 容易受到雨、雷、磁暴等自然现象的影响。

5.4.2 微波

微波是指频率为300MHz~300GHz的电磁波,是无线电波中一个有限频带的简称,即波长在1m(不含1m)到1mm之间的电磁波,是分米波、厘米波和毫米波的统称。微波频率比一般的无线电波频率高,通常也称为超高频电磁波。

微波传输优势主要表现在:

(1) 微波波段频带宽,容量大。

(2) 微波具有直线传播性,并具有近似光波的传播特性。

(3) 由于微波波长很短,天线尺寸小,方向性很强,电磁波能量集中,可以实现低功率远距离传输。

(4) 微波受工业、天电和宇宙等外部干扰影响小,通信质量稳定可靠。

微波通信早期以模拟系统为主,主要用于远距离传输,作为干线传输的重要手段。例如卫星广播传输和城市间的电视节目传输主要依靠的就是微波传输。

5.4.3 红外线

在太阳光谱中,红外线可以用作传输媒介。红外通信技术,在世界范围内是被广泛使用的一种无线通信技术。太阳光谱上红外线的波长大于可见光线,波长为0.75~1000μm。红外线可分为3部分,即近红外线,波长为0.75~1.50μm;中红外线,波长为1.50~6.0μm;远红外线,波长为6.0~1000μm。

红外通信技术适合于低成本、跨平台、点对点高速数据连接,在计算机网络通信中占有重要地位。其主要应用是设备互联和信息网关。设备互联后可完成不同设备内文件与信息的交换。信息网关负责连接信息终端和互联网。

红外通信技术特点主要如下：

(1) 通过数据电脉冲和红外光脉冲之间的相互转换实现无线的数据收发。

(2) 主要是用来取代点对点的线缆连接。

(3) 小角度(30°锥角以内)、短距离、点对点直线数据传输，保密性强。

(4) 传输速率较高，16Mbps 速率的 VFIR 技术已成熟。

(5) 使用不透光材料的阻隔性，可以在不同的物理空间里使用。

(6) 无频道资源占用性，安全特性高。

(7) 具有优秀的互换性和通用性。红外线发射和接收设备在同一频率的条件下可以相互使用。

(8) 红外线是一种对人体有益的光谱，所以红外线产品是绿色产品。

5.5 本章小结

常用的传输介质分为有线传输介质和无线传输介质两大类。有线传输介质中，双绞线可分为屏蔽双绞线(STP)和非屏蔽双绞线(UTP)；与双绞线相比，同轴电缆的抗干扰能力强，屏蔽性能好，传输数据稳定，价格也便宜，根据传输频带的不同，同轴电缆可分为基带同轴电缆和宽带同轴电缆两种类型；光纤由纤芯、包层和涂覆层 3 部分组成。

无线传输介质是利用可以穿越外太空的大气电磁波来传输信号的。无线传输介质具有不受地理条件的限制、建网速度快等特点，目前应用于计算机无线通信的手段主要有无线电短波、微波、红外线、激光以及卫星通信等。

综合训练

一、理论题

1. 选择题

(1) 基带同轴电缆阻抗为(　　)。

A. 100Ω　　B. 50Ω　　C. 75Ω　　D. 150Ω

(2) 非屏蔽双绞线电缆用色标来区分不同的线，计算机网络系统中常用的 4 个绞线对有 4 种颜色，它们是(　　)。

A. 蓝色、橙色、绿色和紫色　　B. 蓝色、红色、绿色和棕色

C. 蓝色、橙色、绿色和棕色　　D. 白色、橙色、绿色和棕色

(3) 单模光纤纤芯直径较细，通常在(　　)范围内。

A. 8.3～125μm　　B. 62.5～125μm　　C. 50～125μm　　D. 8～10μm

(4) 在地形较复杂的地区，传输介质宜选用(　　)。

A. 双绞线　　B. 同轴电缆　　C. 光纤　　D. 无线传输

2. 填空题

（1）常用的传输介质分为________和________两大类。
（2）通常双绞线有________个绞对，共________芯。
（3）同轴电缆从用途上分可分为________同轴电缆和________同轴电缆。
（4）光纤按传输模式可分为________和________两类。
（5）无线电波是指在自由空间传播的________的________波。

3. 简答题

（1）传输介质如何分类？
（2）什么是 UTP 和 STP？
（3）试比较同轴电缆、双绞线和光缆的优缺点。
（4）光纤的纤芯直径有哪些？

二、实践题

1. 制作 UTP 双绞线

（1）实践材料：UTP 超五类（CAT-5e）双绞线 0.5～1.5m、RJ-45 水晶头两个，专用压线钳一把，测线仪一个，见图 5-7。



图 5-7　双绞线制作工具

① RJ-45 连接器包括插头（RJ-45 头）和插座（RJ-45 模块）。一般情况下 RJ-45 模块安装在机器设备上，而双绞线的两端是 RJ-45 头。

② 压线钳主要用于施工中将双绞线按所需切割分段，以及外皮的分离和水晶头的压制。

③ 测线仪主要用于双绞线制作完成后的连通性测试。

（2）关于双绞线制线标准，国际采用 EIA/TIA-568 A（即 T568A）与 EIA/TIA-568 B（T568B）标准。两种制线标准排线顺序详见表 5-3。

表 5-3　T568A 与 T568B 排线顺序标准

制线标准	1	2	3	4	5	6	7	8
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

(3) 在以太网中，根据双绞线使用场合的不同，UTP 双绞线分为直通线和交叉线两种。直通线和交叉线两端的线序是不同的，如图 5-8 和图 5-9 所示。

引脚	颜色	信号	信号	颜色	引脚
1	白橙	TD+	RD+	白橙	1
2	橙	TD−	RD−	橙	2
3	白绿	RD+	TD+	白绿	3
4	蓝			蓝	4
5	白蓝			白蓝	5
6	绿	RD−	TD−	绿	6
7	白棕			白棕	7
8	棕			棕	8

图 5-8　直通线线序

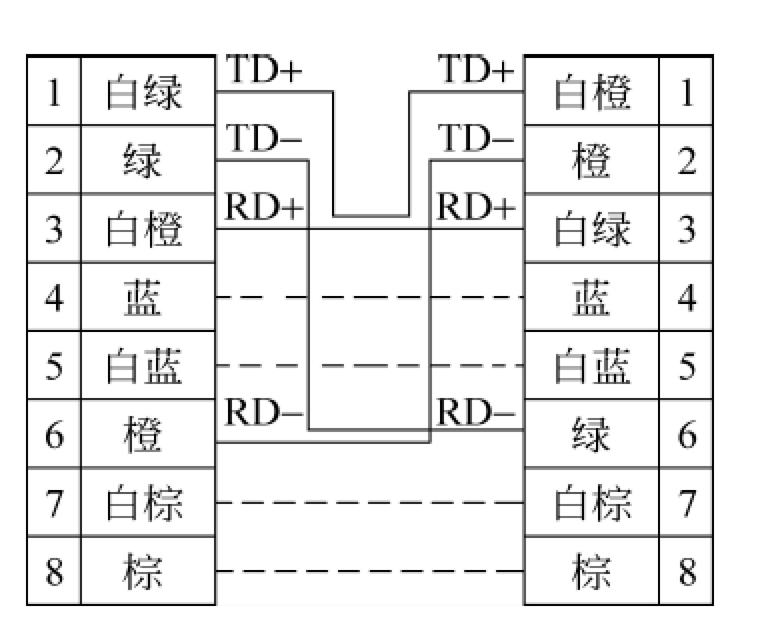


图 5-9　交叉线线序

(4) 直通线与交叉线的适用场合。

直通线适用于以下条件：

① 主机与交换机的普通端口连接。

② 交换机与路由器的以太网端口相连。

③ 集线器的 uplink 端口与交换机的普通端口相连。

交叉线适用于以下条件：

① 主机与主机的网卡端口连接。

② 交换机与交换机的非 uplink 端口相连。

③ 路由器的以太网端口互连。

④ 主机与路由器以太网端口相连。

(5) 制作一条 UTP 交叉线，参考步骤如下。

① 准备制作网线设备与材料，如图 5-10 所示。



图 5-10　制作设备材料

② 使用压线钳的剥线孔，剥去双绞线外面的橡胶层，注意不要伤及绞线，如图 5-11 所示。




图 5-11 剥去外层

③ 按制线标准捋出线序，如图 5-12 所示。




图 5-12 捋线

④ 将捋好的线剪齐，然后平稳地插入水晶头内，如图 5-13 所示。

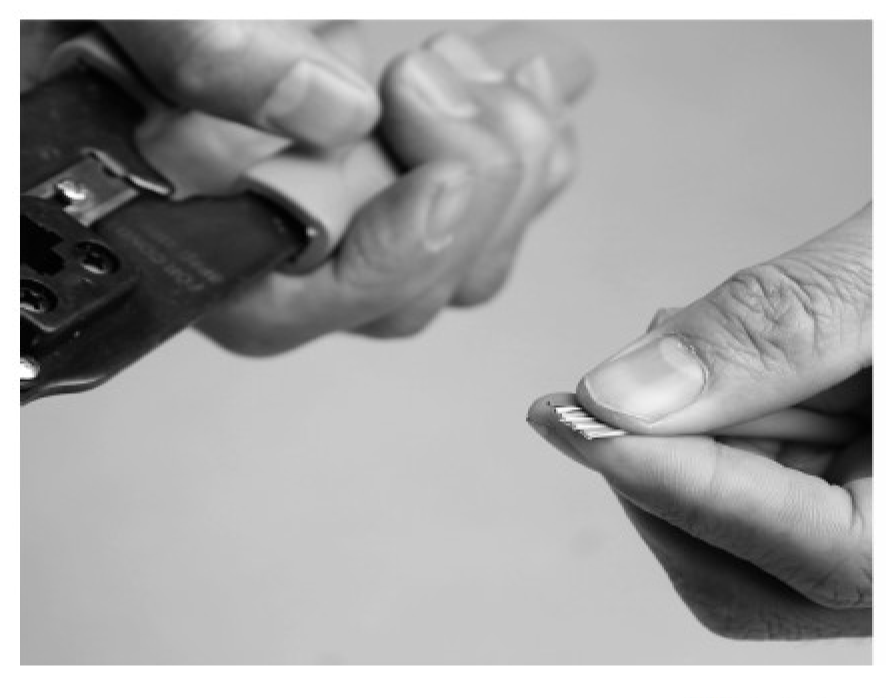



图 5-13 插入水晶头

⑤ 网线与水晶头相向用力，确保线头插入水晶头底部，如图 5-14 所示。

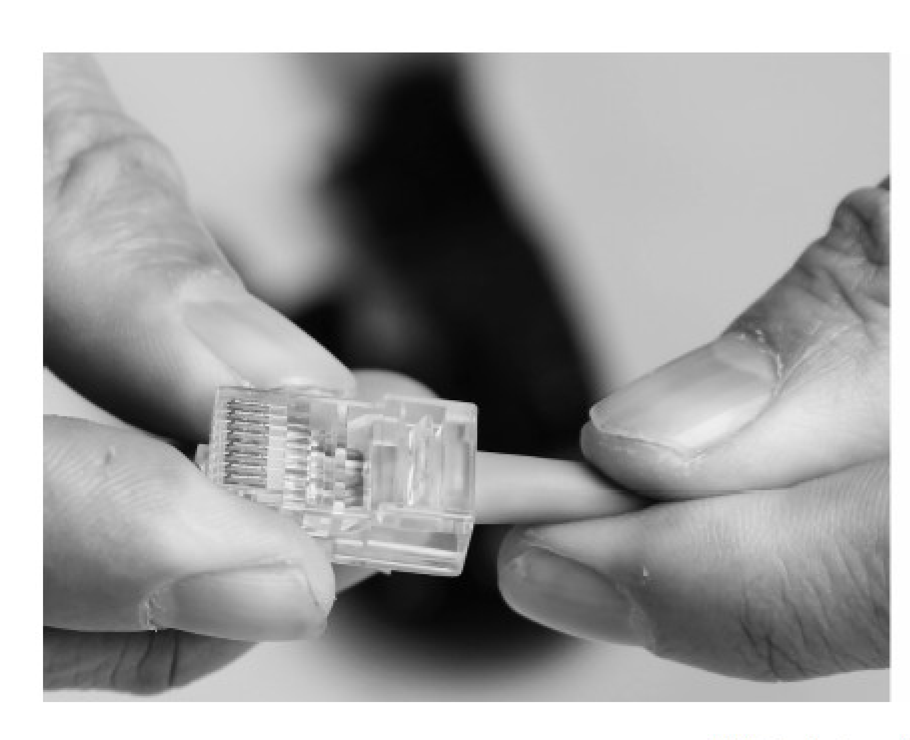
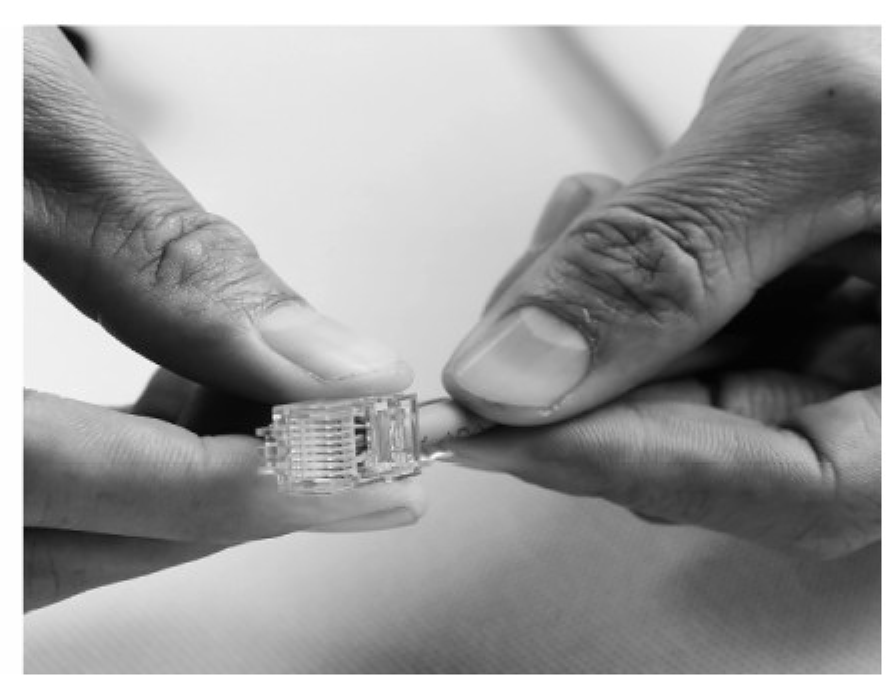



图 5-14　插紧水晶头

⑥ 将水晶头平稳放入压线钳的水晶头压制孔，用力完成压线操作，如图 5-15 所示。

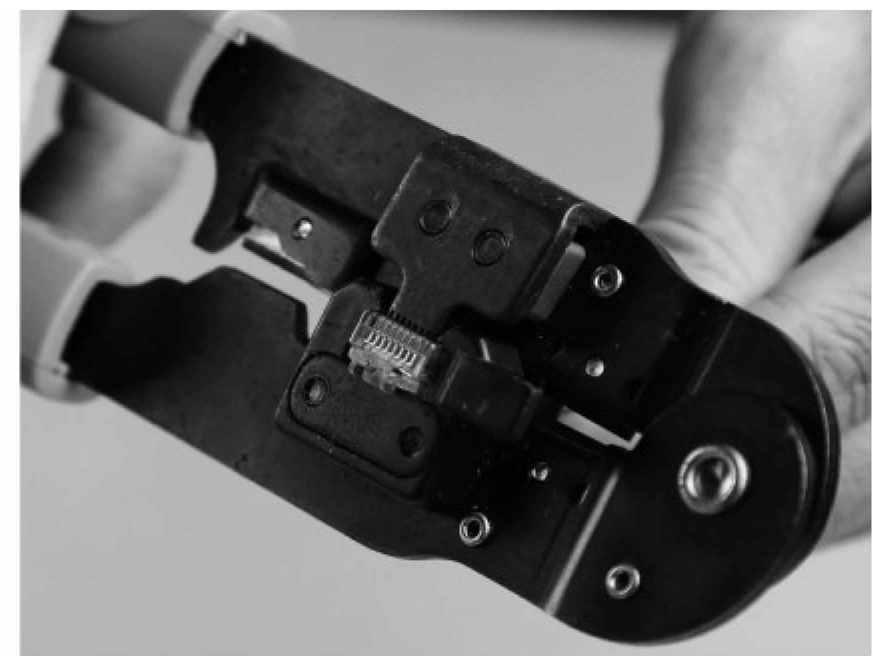



图 5-15　压线

⑦ 重复②～⑥步骤，完成一条网线制作。对制作完成的网线进行连通性测试，如图 5-16 所示。




图 5-16　网线测试

2. 完成双机直连通信实验

完成双机直连通信实验如图 5-17 所示。



图 5-17 双机直连示意

参考步骤如下：

(1) 安装网卡驱动。

Windows XP 以上操作系统支持大多数网卡，网卡驱动一般不需要安装。

(2) 安装通信协议。

进入“网络连接”，双击“本地连接”，在弹出的窗口中选择“属性”，进入网络协议管理与设置窗口，单击“安装”或“删除”来添加或删除网络协议。

(3) 设置 IP 地址。

在“本地连接 属性”窗口中选择“Internet 协议(TCP/IP)”，设置“IP 地址”、“子网掩码”以及“网关”，将两台计算机设在一个网段中。

(4) 设置标识。

两台计算机的标识要不同。在“系统属性”的“计算机名”中进行设置，只需要单击“更改”按钮，更改后单击“确定”按钮，再重启即可。

(5) 设置共享资源。

在一台或两台计算机上分别设置共享资源。

(6) 访问共享资源。

通过“网上邻居”或者查找计算机，就可以访问对方的共享资源。

第 6 章　网络设备及功能

本章主要内容

- 网络适配器
- 调制解调器
- 中继器和集线器
- 交换机和路由器

网络设备是指连接计算机网络的实体物理媒体。网络设备的种类繁多，功能各异，发展日新月异。在计算机网络的组建过程中，常用的网络设备除了计算机之外，主要是连接设备，有网络适配器、调制解调器、中继器、集线器、网桥、交换机和路由器等。了解这些设备的工作原理和功能可以让我们对计算机网络有更深刻的理解。

6.1　网络适配器

网络适配器（Network Interface Card，NIC，也称网络接口卡，俗称网卡），见图 6-1，网卡是局域网中最基本的部件之一，它是连接计算机与网络的硬件设备。无论是双绞线连接、同轴电缆连接还是光纤连接，都必须借助于网卡才能实现数据的通信。



(a) AUI接口网卡　　(b) RJ-45接口网卡　　(c) 移动网卡

图 6-1　网络适配器

6.1.1　工作原理

网络卡的内核是链路层控制器，该控制器通常能实现多链路层服务，这些服务包括成帧、链路接入、流量控制、差错检测等。此外，由于局域网上传送的数据速率与计算机总线的数据速率是不一样的，网卡的另一个作用就是缓存数据，以调整它们之间的速率匹配问题。

6.1.2 功能特征

每块网卡都有一个唯一的网络节点地址，它是网卡生产厂家在生产时烧入 ROM 只读存储芯片中的，称为 MAC 地址或物理地址，在全球范围内 MAC 地址唯一。

网卡按传输速度可分为 10Mbps 网卡、10/100Mbps 自适应网卡以及千兆(1000Mbps)网卡等。

按总线类型可分为 ISA、EISA、VESA、PCI 和 PCMCIA 等。

按网络接口可分为适用于以太网的 RJ-45 接口、细同轴电缆 BNC 接口、粗同轴电缆 AUI 接口、FDDI 接口和 ATM 接口等的网卡。

按传输方式分为有线网卡与无线(移动)网卡。

PC 使用的网卡多数是在计算机主板上集成了 PCIE 总线、RJ-45 接口的以太网网卡。随着移动 PC 的不断普及，移动网卡将会逐步成为主流。

6.2 调制解调器

调制解调器(modem)，即能将数字信号转换成模拟信号在模拟信道上传送，也能将接收到的模拟信号转换成数字信号的设备，如图 6-2 所示。目前，较多的家庭 PC 是通过公用电话网接入计算机网络的，因而需通过调制解调器进行上述转换。



图 6-2 调制调解器

6.2.1 工作原理

调制解调器是为数字信号在具有有限带宽的模拟信道上进行远距离传输而设计的，它一般由基带处理、调制解调、信号放大和滤波、均衡等几部分组成。调制是将数字信号与载波叠加，产生适合于在信道上传输的模拟信号；解调是从模拟信号中恢复出数字信号。

6.2.2 ADSL 调制调解器简介

调制解调器的性能及速率直接关系到联网以后传输信息的速度，目前，调制解调器的速率以 56kbps 使用较为普遍。ADSL 调制调解器(ADSL modem)也叫做 DSL 调制调解器，ADSL 技术是一种不对称数字宽带接入互联网技术，ADSL 充分利用现有的铜线资源，可以在一对双绞线上提供上行 640kbps、下行 8Mbps 的带宽。

6.3 中继器

中继器(repeater),是在物理层上实现局域网网段互联的设备,是最简单的网络互联设备,负责连接各个电缆段,对信号进行放大和整形,用来驱动长线电缆,起到在不同电缆段间复制信号的作用,如图 6-3 所示。



(a) 有线中继器　　(b) 无线中继器

图 6-3　中继器

6.3.1 工作原理

传输线路由于受噪声的影响,承载信息的数字信号或模拟信号只能传输有限的距离,中继器的功能是对接收信号进行再生和发送,从而增加信号传输的距离。中继器适用于完全相同的两类网络的互联,主要功能是通过对数据信号的重新发送或者转发,放大信号,补偿信号衰减,来扩大网络传输的距离。

6.3.2 功能特征

中继器是最简单的网络互联设备,连接同一个网络的两个或多个网段。如以太网常常利用中继器扩展总线的电缆长度,标准细缆以太网的每段长度最大为 185m,最多可有 5 段,因此增加 4 个中继器后,最大网络电缆长度则可提高到 925m。

一般来说,中继器两端的网络部分是网段而不是子网。中继器可以连接两个局域网间的电缆,重新定时并再生电缆上的数字信号,然后发送出去。

6.4 集线器

集线器(hub)属于数据通信系统中的基础设备,是一种不需任何软件支持或只需很少管理软件管理的硬件设备,广泛应用于组建共享网络,如图 6-4 所示。



图 6-4　集线器

6.4.1　工作原理

集线器内部采用了电器互联，在这方面，集线器所起的作用相当于多端口的中继器。集线器实际上就是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又称为多口中继器。

集线器上有多个端口，能将各个电缆段连接在一起，而它则成为网络中的一个中心节点。集线器工作于 OSI 参考模型的第一层（物理层），以广播模式工作，所有的端口都共享一条带宽。

6.4.2　功能特征

集线器主要用于共享网络的组建，是解决从服务器直接到桌面的经济方案。在交换式网络中，集线器直接与交换机相连，将交换机端口的数据送到桌面。使用集线器组网灵活，它是网络中的一个星形节点，对节点相连的工作站进行集中管理。当传输的内容不涉及语音和图像，传输量相对较小时，选择 10Mbps 的集线器即可；如果传输量较大，且有可能涉及多媒体应用，如语音信号时，应当选择 100Mbps 或 10/100Mbps 自适应集线器。随着交换机价格大幅降低，集线器已逐步被交换机取代。

6.5　交换机

交换机（switch）是一种用于电信号转发的网络设备，如图 6-5 所示。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。其主要作用是在连接到广域网带宽



图 6-5　交换机

上时进行语音、数据资料及视频通信。交换机通常在OSI参考模型的数据链路层上运行。

随着计算机网络的飞速发展，出现了各种类型的交换机，对交换机的分类也比较困难，一般分类如下。

(1) 按交换机所支持的局域网标准分类：

① 以太网交换机。

② FDDI交换机。

③ ATM交换机。

④ 令牌环交换机。

(2) 按交换机的架构分类：

① 单台交换机。交换机单独使用，不可堆叠。

② 堆叠交换机。将多个单台可堆叠交换机连接在一起，构成一个整体。

③ 箱体模块化交换机。在其扩展槽中可以插入各种局域网标准、各种介质接口的交换模块。

(3) 按交换机工作在OSI参考模型的层次分类：

① 工作在数据链路层的第二层交换机。

②工作在网络层的第三层交换机。

③ 工作在传输层的第四层交换机。

④ 多层交换机。

本节对以太网交换机工作协议层划分的第二层交换机、第三层交换机和第四层交换机进行简单介绍。

6.5.1 交换机概述

以太网交换机是基于以太网传输数据的交换机，以太网采用共享总线型传输媒体方式的局域网。以太网交换机的结构是每个端口都直接与主机相连，并且一般都工作在全双工方式。交换机能同时连通许多对端口，使每一对相互通信的主机都能像独占通信媒体那样无冲突地传输数据。

以太网交换机应用最为普遍，价格也较便宜，因此，它是构建局域网的主要联网设备，以太网交换机通常都有几个到几十个端口，端口速率可以不同，工作方式也可以不同，如可以提供10Mbps、100Mbps等带宽，提供半双工、全双工和自适应的工作方式等。

6.5.2 第二层交换机

第二层交换机是用来取代集线器的设备，特别是在高速局域网环境下。第二层交换机有时也被称为交换集线器。第二层交换机属于数据链路层设备，可以识别数据包中的MAC地址信息，根据MAC地址进行转发，并将这些MAC地址与对应的端口记录在其内部的一个地址表中。

其工作原理如下：

(1) 当交换机从某个端口收到一个数据包时，先读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的计算机是连在哪个端口上。

(2) 读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

(3) 如表中有与该目的 MAC 地址对应的端口，把数据包直接复制到该端口上。

6.5.3 第三层交换机

随着计算机网络设备数量不断增加，第二层交换机显露出广播超负荷和缺少多链路等问题。为此，出现了第三层交换机，它在硬件上实现了路由器的分组转发功能。

目前，市场上有多种不同的第三层交换机，分组式交换是第三层交换机的主要类型。分组式交换机与传统路由器的操作方式相同。由于转发逻辑由硬件实现，与基于软件的路由器相比，分组式交换机在性能上呈几何级数增长。

第三层交换技术简单地说就是第二层交换技术与第三层转发技术的结合。它改变了局域网中网段划分之后网段的中子网必须依赖路由器进行管理的局面，解决了传统路由器低速、复杂所造成的网络瓶颈问题。

第三层交换机的工作原理是：交换机在对第一个数据流进行路由后，将会产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不需再次路由，从而消除了路由器进行路由选择而造成的网络延迟，提高了数据包转发的效率。

6.5.4 第四层交换机

第四层交换机是工作于 OSI 参考模型的第四层，即传输层，直接面对具体应用的设备。

如前所述，第二层交换机依赖于 MAC 地址完成链路层信息交换，第三层交换机则将 IP 地址信息用于网络路径选择来完成信息交换。而第四层交换机则是用传输层数据包的包头信息来帮助信息交换和传输处理的。也就是说，第四层交换机的交换信息所描述的具体内容实质上是包含在每个 IP 包中的所有协议或进程，如用于 Web 传输的 HTTP，用于文件传输的 FTP，用于终端通信的 Telnet，用于安全通信的 SSL 等协议。这样，在一个 IP 网络里，普遍使用的第四层交换协议实质就是基于 TCP/UDP 协议。

由于 TCP 和 UDP 数据包的包头不仅包括了端口号信息，还指明了正在传输的数据包是什么类型的网络数据，使用这种与特定应用有关的信息，就可以完成大量的网络数据传输和交换的质量服务，第四层交换机普遍采用的主要技术包括包过滤/安全控制、服务质量、服务器负载均衡和主机备用连接等。

第四层交换技术相对于原来的第二层、第三层交换技术具有明显的优点。第四层交换机不仅可以完成端到端交换，还能识别传输层协议端口，依照特定应用提供质量服务。

6.6 路由器

路由器(router)是连接因特网中各局域网和广域网的设备,它会根据信道的情况自动选择和设定路由,以最佳路径,按前后顺序发送信号。路由器如图 6-6 所示。



图 6-6 路由器

6.6.1 工作原理

路由器内部有一个路由表,标明了如果要去某个地方则下一步应该往哪走。路由器从某个端口收到一个数据包后,首先把链路层的包头去掉(拆包),读取目的 IP 地址,然后查找路由表,若能确定下一步的地址,则再加上链路层的包头(打包),把该数据包转发出去;如果不能确定下一步的地址,则向源地址返回一个信息,并把这个数据包丢掉。

路由技术和交换看起来有点相似,其实路由和交换之间的主要区别就是交换发生在 OSI 参考模型的第二层(数据链路层),而路由发生在第三层。这一区别决定了路由和交换在传送数据的过程中需要使用不同的控制信息,所以两者实现各自功能的方式是不同的。

6.6.2 路由技术

路由技术由两项最基本的活动组成,即决定最优路径和传输数据包。其中,数据包的传输相对较为简单和直接,而路由的确定则更加复杂一些。路由算法在路由表中写入各种不同的信息,路由器会根据数据包所要到达的目的地,选择最佳路径把数据包发送到可以到达该目的地的下一台路由器处。当下一台路由器接收到该数据包时,也会查看其目标地址,并使用合适的路径继续传送给后面的路由器。依次类推,直到数据包到达最终目的地。

路由选择算法可以分为静态路由选择算法和动态路由选择算法。

路由器主要用于不同类型的网络之间。它最主要的功能就是路由转发,解决好各种

复杂路由路径网络的连接就是它的最终目的，所以路由器的路由功能通常非常强大，不仅适用于同种协议的局域网间，更适用于不同协议的局域网与广域网间。它的优势在于选择最佳路由、负荷分担、链路备份及和其他网络进行路由信息的交换等功能。路由器通过分析其他路由器发出的路由更新信息，可以掌握整个网络的拓扑结构。另外，路由器为了与各种类型的网络连接，有非常丰富接口类型。

6.7 本章小结

本章介绍了常见的网络设备及其功能，其中，网卡是局域网中最基本的部件之一，它是连接计算机与网络的硬件设备。无论是双绞线连接、同轴电缆连接还是光纤连接，都必须借助于网卡才能实现数据的通信；由于信号在网络介质传输中有衰减和噪声，使有用的信号变得越来越弱，为了保证有用数据的完整性，并在一定范围内传送，要用中继器把接收到的弱信号放大以保持与原数据相同；集线器属于数据通信系统中的基础设备，应用于OSI参考模型的第一层，因此又被称为物理层设备。交换机是一种用于电信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。根据以太网交换机工作协议层划分为第二层交换机、第三层交换机和第四层交换机。路由器的主要功能就是进行路由选择。当一个网络中的主机要给另一个网络中的主机发送分组时，它首先把分组送给同一网络中用于网间连接的路由器，路由器根据目的地址信息选择合适的路由，该分组最后被递交给目的主机。

综合训练

一、理论题

1. 选择题

(1) 全球每块网卡都有一个唯一的网络节点地址，该地址称为(　　)。
A. IP地址　　B. 编码地址　　C. MAC地址　　D. ROM

(2) 目前PC网卡的网络接口为(　　)。
A. RJ-45　　B. BNC　　C. AUI　　D. FDDI

(3) 细缆增加4个中继器后，最大网络电缆长度则可提高到(　　)m。
A. 100　　B. 925　　C. 185　　D. 150

(4) 二层交换将MAC地址与对应的端口记录在自己内部的一个(　　)中。
A. MAC　　B. IP　　C. ROM　　D. 地址表

(5) 路由器一般工作在OSI参考模型的(　　)。
A. 数据链路层　　B. 物理层　　C. 网络层　　D. 应用层

2. 填空题

(1) 网卡的内核是________控制器，该控制器通常实现多________。

(2) 中继器是最简单的网络互联设备,连接同一个网络的________网段。
(3) 第二层交换机属________层设备,可以识别数据包中的________信息。
(4) 第四层交换机是工作于 OSI 参考模型的________传输层。
(5) 路由选择算法可以分为________选择算法和________ 选择算法。

3. 简答题

(1) 简述网卡的工作原理以及网络接口特征。
(2) 简述 ADSL 调制调解器基本特性。
(3) 简述二层交换机工作原理。
(4) 简述路由器工作原理。

二、实践题

1. 以太网交换机的基本配置

以 Cisco C2950 交换机为例,完成对交换机主机名称(设为 sunline)与登录口令(设为 123456)设置。

参考步骤如下:

(1) 通过 Console 电缆把 PC 的 COM 端口和交换机的 Console 端口连接起来,如图 6-7 所示。

(2) 设置 PC 为超级终端,设置 COM 通信参数如下:波特率为 9600bps,8 位数据位,1 位停止位,无校验和无流控,并选择终端类型为 VT100,如图 6-8 所示。



图 6-7 连接示意图



图 6-8 设置 COM 通信参数

(3) 给交换机加电,等待交换机启动,如图 6-9 所示。

(4) 交换机启动完毕,进入交换机用户模式。

在交换机用户模式中,可以对交换机进行有限操作,如显示软、硬件版本和进行简单

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by miwang
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.

2950-24 starting...
Base ethernet MAC Address: 0030.A344.5311
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 3058048
flashfs[0]: Bytes available: 60958336
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2950-i6q4l2-mz.121-22.EA4.bin"...
########################################################################## [OK]
              Restricted Rights Legend
```

图 6-9　交换机启动

的测试等操作。

命令提示符格式：

主机名>

Switch>　(用户模式)

(5) 进入交换机特权模式，命令为 enable，可以简写为 en。

交换机特权模式是比用户模式高一级的操作模式，可进行配置文件的管理，查看交换机信息，进行网络测试和调试等，有配置和监视权力，是进入其他配置模式的前提。

命令提示符格式：

主机名#

Switch>enable　(进入特权模式)

Switch#　(特权模式)

(6) 进入交换机全局模式，命令为 configure terminal，可以简写为 conf t。

交换机全局模式是比特权模式高一级的操作模式，可配置交换机的全局性参数，如主机名、登录信息等内容。

命令提示符格式：

主机名(config)#

Switch# configure terminal　(进入全局模式)

Switch(config)#　(全局模式)

例如：

Switch(config)#hostname sunline　(设置交换机名称为 sunline)

S2950(config)#enable password 123456　(设置交换机登录口令为 123456)

(7) 进入交换机端口模式，命令为 interface f0/x，可以简写为 int f0/x，其中 x 指端口号。

在交换机端口模式可以进入下一级配置，对交换机的端口进行参数配置。

命令提示符格式：

主机名(config-if)#

```
Switch(config)#interface f0/x   (进入端口模式)
Switch(config-if)#              (端口模式)
```

(8) 基本配置完成，如图 6-10 所示。

```
Press RETURN to get started!


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sunline
sunline(config)#enable password 123456
sunline(config)#int f0/19
sunline(config-if)#exit
sunline(config)#
```

图 6-10　配置完成

2. 路由器的基本配置

以 Cisco C2621 路由器为例，完成路由器的名称和登录密码(密文)等基本配置。

连接如图 6-11 所示。设置 PC 为超级终端，设置 COM 通信参数为：波特率为 9600bps，8 位数据位，1 位停止位，无校验和无流控。



图 6-11　连接示意图

参考步骤如下：

(1) 通过 Console 电缆把 PC 的 COM 端口和路由器的 Console 端口连接起来。

(2) 各命令状态如下。

① router>

路由器处于用户命令状态，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

② router#

在 router>提示符下输入 enable，路由器进入特权命令状态，提示符为 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

③ router(config)#

在 router#提示符下输入 configure terminal，出现提示符 router(config)#，此时路由器处于全局设置状态，可以设置路由器的全局参数。

④ router(config-if)#

```
router(config-line)# ;
router(config-router)#
```

路由器处于局部设置状态，这时可以设置路由器某个局部的参数。

⑤ >

路由器处于 RXBOOT 状态，在开机后 60 秒内按 Ctrl+Break 键可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

(3) 设置对话状态。

这是一台新路由器开机时自动进入的状态，在特权命令状态使用 Setup 命令也可进入此状态，这时可通过对话方式对路由器进行设置。利用设置对话过程可以避免手工输入命令的烦琐，但它还不能完全代替手工设置，一些特殊的设置还必须通过手工输入的方式完成。

进入设置对话过程后，路由器首先会显示一些提示信息：

```
---System Configuration Dialog---
At any point you may enter a question mark '? ' for help.
Use Ctrl-C to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

这是告诉用户在设置对话过程中的任何地方都可以输入"?"得到系统的帮助，按 Ctrl+C 键可以退出设置过程，默认设置将显示在"[]"中。然后路由器会问是否进入设置对话：

```
Would you like to enter the initial configuration dialog? [yes]:
```

如果按 y 或按回车键，路由器就会进入设置对话过程。首先可以看到各端口当前的状况：

```
First,would you like to see the current interface summary? [yes]:
Any interface listed with OK? value "NO" does not have a valid configuration
Interface  IP-Address  OK?  Method  Status  Protocol
Ethernet0  Unassigned  NO   unset   up      Up
Serial0    Unassigned  NO   unset   up      up
⋮          ⋮           ⋮    ⋮       ⋮       ⋮
```

然后，路由器就开始全局参数的设置：

```
Configuring global parameters:
```

设置路由器名：

```
Enter host name [Router]:
```

设置进入特权状态的密文(secret)，此密文在设置以后不会以明文方式显示：

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
Enter enable secret: cisco
```

设置进入特权状态的密码(password)，此密码只在没有密文时起作用，并且在设置以后会以明文方式显示：

```
The enable password is used when there is no enable secret
and when using older software and some boot images.
Enter enable password: pass
```

设置虚拟终端访问时的密码：

```
Enter virtual terminal password: cisco
```

询问是否要设置路由器支持的各种网络协议：

```
Configure SNMP Network Management? [yes]:
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]:
Configure RIP routing? [no]:
...
```

3. 家用路由器功能配置

根据家庭网络应用情况，在第 3 章综合训练中的家用路由器设置的基础上，完善家庭路由器的功能配置。

第 7 章　网络操作系统

本章主要内容

- 网络操作系统的功能及特性
- 常用网络操作系统介绍
- 网络操作系统的选择

操作系统(Operating System,OS)是计算机系统的核心组成部分,用来控制与管理计算机软件与硬件资源,为用户提供全面、方便以及可扩展的工作环境,合理地组织计算机软硬件资源完成规定的作业任务,是一个复杂的软件集合。网络操作系统(Network Operating System,NOS)是操作系统和网络通信技术相结合的产物,不但具备操作系统的功能,还具备网络通信功能。

7.1　网络操作系统的功能及特性

7.1.1　操作系统的主要功能

操作系统的管理功能包括处理机管理、存储管理、设备管理、文件管理和接口管理 5 个主要功能。

1. 处理机管理

处理机管理的主要工作是在程序并发执行的情况下,解决处理机分配调度策略、分配实施和资源回收等问题。不同的操作系统对处理机的管理策略是不同的。

2. 存储管理

存储管理的主要工作是对内部存储器进行分配、保护和扩充。存储管理的主要技术有分区存储管理、覆盖交换技术、页式管理和段式与段页式管理等。

3. 设备管理

设备管理的主要工作是对计算机输入输出系统进行管理,选择和分配输入输出设备,控制输入输出设备和 CPU 或内存之间传输数据,为用户提供一个物理透明的、友好的操作接口,提高设备与设备之间、CPU 与设备之间以及进程与进程之间的并行操作度,管理缓冲区的使用。

4. 文件管理

文件管理的主要工作包括存储空间管理、目录管理、文件访问管理和软件管理。存储

空间管理解决如何存放信息以提高空间利用率和读写性能的问题，目录管理解决信息检索方式问题，文件访问管理通过权限授予和用户分类等手段解决文件访问的授权和安全问题，软件管理解决软件的版本区分、安装和卸载问题。

5. 接口管理

接口管理包括程序接口管理和作业接口管理。程序接口管理是一组广义指令（也称系统调用），提供应用程序或其他系统程序的功能调用，例如数据传输请求、文件操作请求等。作业接口管理也是一组控制操作命令，让用户去组织和控制自己的作业运行。

7.1.2 操作系统的主要特性

操作系统有并发性、共享性、虚拟性和封闭性4个主要的特性。

1. 并发性

并发性是指计算机系统中程序的并发执行，即一组在逻辑上互相独立的程序或程序段在执行过程中其执行时间在客观上互相重叠的特性。从宏观角度看，程序是并行执行；从微观角度来看，程序是串行执行。

2. 共享性

共享性是指计算机系统中的各种软硬件资源由各个并发程序共享使用。这种资源的共享性，使得操作系统必须采用某种有效策略合理地分配资源，解决资源竞争问题。

3. 虚拟性

虚拟性是指把物理上的一台设备变成逻辑上的多台设备，如操作系统采用多道程序并发执行的技术，把一台计算机变成逻辑上的多台计算机同时给多个用户使用。

4. 封闭性

封闭性是指一个程序在初始条件相同的情况下，无论何时运行，其执行结果都一样。

7.1.3 网络操作系统的功能与特点

网络操作系统承担网络用户与计算机网络之间的控制管理，网络操作系统除了具备上述操作系统的基本功能与特点外，还应具有如下主要的网络支持功能和特点。

1. 网络操作系统的两大功能

1）网络通信

网络操作系统应保障计算机网络具有高效、可靠的网络通信能力。

2）网络服务

网络操作系统能为计算机网络提供多种网络服务功能，如远程作业录入并进行处理的服务功能、文件传输服务功能、电子邮件服务功能和远程打印服务功能等。

2. 网络操作系统的特点

1）硬件无关性

网络操作系统与计算机网络内的硬件设备无关，能跨越不同技术类型的网络，能操作网络内不同类型的网络硬件设备，能支持不同规模的计算机系统。

2）支持不同类型的客户端

网络操作系统能支持网络内不同类型的客户端，如 DOS、Windows、UNIX、Linux 和 AppleTalk 等客户端操作系统。

3）网络目录服务

网络操作系统对网络中不同类型的信息资源进行存储、组织和提供信息访问服务，并支持多用户访问和多任务操作。

4）网络管理与安全控制

网络操作系统对网络通信服务进行监督、组织和控制，实现访问控制、性能检测、网络状态监视、故障检测和计费等功能。

5）系统容错能力

网络操作系统应能提供多级系统容错能力，包括日志式的容错特征列表、可恢复文件系统、磁盘镜像、磁盘扇区备用以及对不间断电源（UPS）的支持。

3. 网络操作系统的工作模式

1）客户/服务器（client/server）模式

在客户/服务器模式下，在网络服务器上安装专门的服务器版操作系统，其中包括大量的服务程序和服务支撑软件。服务器作为网络的控制和管理中心。在客户机上安装工作站网络软件，用于处理本地操作和访问服务器，从服务器获取处理后的数据。

2）对等（peer-to-peer）模式

对等模式网络是将对等模式的网络操作系统和通信协议装入所有接入网络的计算机，这些计算机既作为服务器向其他站点提供服务，又作为工作站接受其他站点的服务，各计算机地位平等、资源共享。网络中没有服务处理中心，也没有控制中心。

一般网络操作系统的工作模式是客户/服务器模式。

7.2 常用网络操作系统介绍

网络操作系统的种类很多，但是根据其各自的特点和优势，应用的范围和场合不尽相同，主要有微软公司的 Windows 系列产品，Novell NetWare 操作系统，UNIX 和 Linux 等几种。

7.2.1 UNIX 操作系统

UNIX 是 20 世纪 70 年代初出现的一个操作系统，除了作为网络操作系统之外，还可以作为单机操作系统使用，目前主要用于工程应用和科学计算等领域。其特点如下。

(1) 安全可靠。UNIX 在系统安全方面是任何一种操作系统都不能与之相比的，很少有计算机病毒能够侵入。这是因为 UNIX 一开始就是为多任务、多用户环境设计的，在用户权限、文件和目录权限、内存等方面有严格的规定。近几年，UNIX 操作系统以其良好的安全性和保密性证实了这一点。

(2) 方便接入 Internet。UNIX 是 Internet 的基础，TCP/IP 协议也是随之发展并完善的。目前的一些 Internet 服务器和一些大型的局域网都使用 UNIX 操作系统。

UNIX 虽然具有许多其他操作系统所不具备的优势，如工作环境稳定、系统的安全性好等，但是其安装和维护对普通用户来说比较困难。

7.2.2 自由软件 Linux

Linux 最初是由芬兰赫尔辛基大学的大学生林纳斯·本纳迪克特·托瓦兹(Linus Benedict Torvalds)于 1991 年 8 月开发的一个免费的操作系统，是一个类似于 UNIX 的操作系统。Linux 涵盖了 UNIX 的所有特点，而且还融合了其他操作系统的优点，如真正支持 32 位和 64 位多任务、多用户虚拟存储、快速 TCP/IP、数据库共享等特性。Linux 的主要特点如下。

(1) 开放的源代码。Linux 许多组成部分的源代码是完全开放的，任何人都可以通过 Internet 得到、开发并发布。

(2) 支持多种硬件平台。Linux 可以运行在多种硬件平台上，还支持多处理器的计算机。

(3) 对外部设备的支持。目前在计算机上使用的大量外部设备 Linux 均支持。

(4) 支持 TCP/IP 等协议。在 Linux 中可以使用所有的网络服务，如网络文件系统、远程登录等。SLIP 和 PPP 支持串行线上的 TCP/IP 协议的使用，用户可用一个高速调制解调器通过电话线接入 Internet。

(5) 支持多种文件系统。Linux 目前支持的文件系统有 FAT16、FAT32、NTFS、EXT2、XIAFS、ISOFS 和 HPFS 等 32 种之多，其中最常见的是 EXT2，其文件名最长可达 255 个字符。

7.2.3 Novell NetWare 操作系统

NetWare 网络操作系统由美国 Novell 公司开发，是多任务、多用户的网络操作系统，它的较高版本提供系统容错能力。它使用开放协议技术，各种协议的结合使不同类型的工作站可与公共服务器通信。这种技术满足了广大用户在不同种类的网络间实现互相通

信的需要，实现了各种不同网络的无缝通信，即把各种网络协议紧密地连接起来，可以方便地与各种小型、中型和大型机连接通信。

NetWare 可以不用专用服务器，任何一种 PC 均可作为服务器。NetWare 操作系统对无盘站和游戏的支持较好，常用于教学网和游戏厅。

7.2.4 Windows 系列操作系统

微软(Microsoft)公司开发的操作系统不仅在单机操作系统中占有绝对优势，在网络操作系统中也具有非常强的力量。图 7-1 给出了微软网络操作系统的发展路线图。

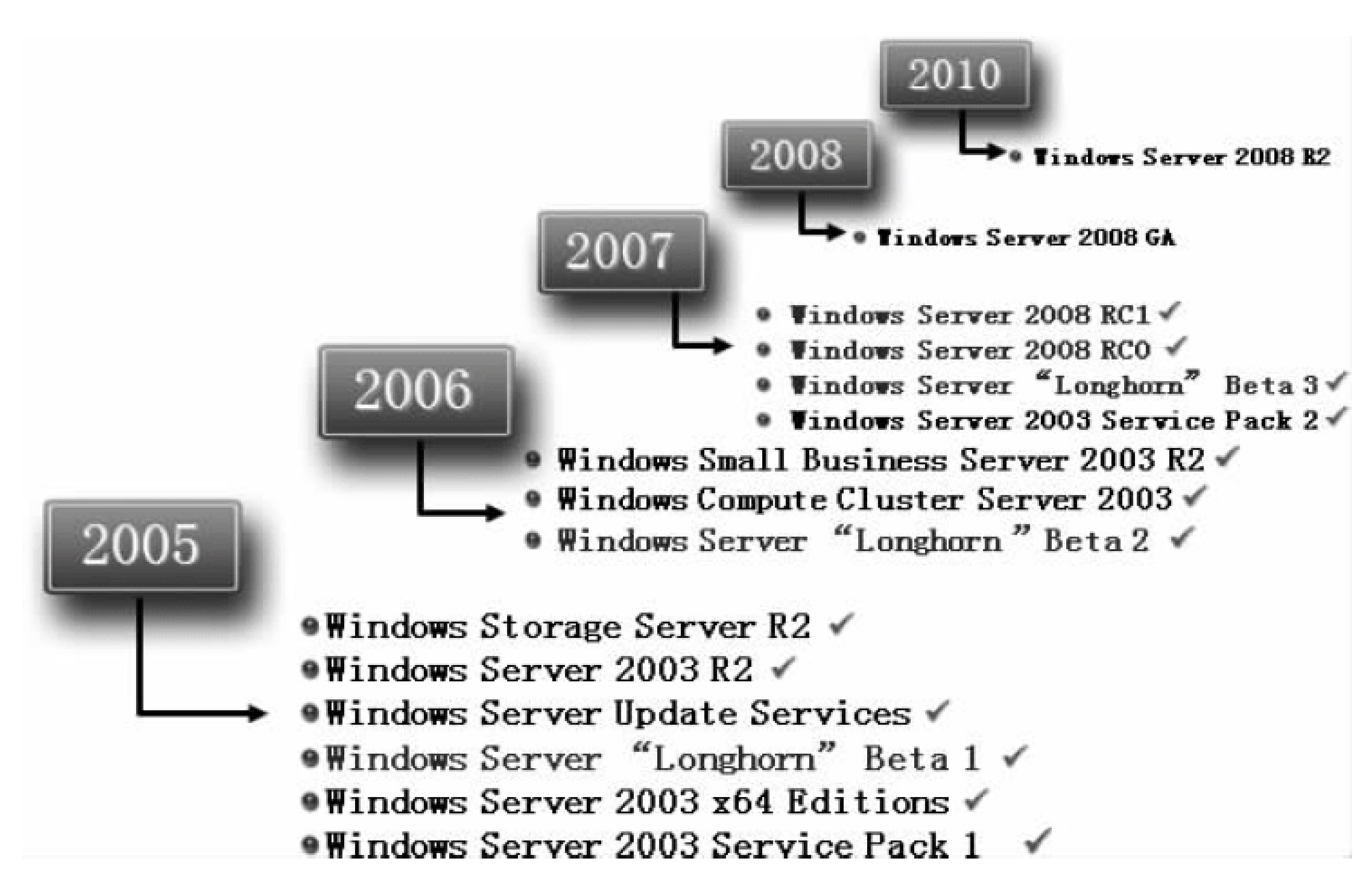


图 7-1 微软公司网络操作系统发展路线图

微软公司在 1993 年推出了面向工作站、网络服务器和大型计算机的网络操作系统——Windows NT。它与通信服务紧密集成，基于 OS/2 NT 核心开发，早期的 Windows NT 系列有 3.1/3.5/3.51/4.0 版。

微软公司于 1999 年 12 月 12 日推出基于 Windows NT 核心的 Windows 2000 系列操作系统。Windows 2000 有 4 个版本：Professional、Server、Advanced Server 和 Datacenter Server。其中，Windows 2000 Server 是服务器版本，它的前一个版本是 Windows NT 4.0 Server 版，面向中小型的企业内部网络服务器，但它同样可以应付企业、公司及大型网络中的各种应用程序的需要。Server 版在 Windows NT 4.0 的基础上做了大量的改进，在各种功能方面有了更大的提高。Advanced Server 版是 Server 版的企业版，具有更为强大的特性和功能，例如，它对多处理器的支持要比 Server 版更好，支持的数目可以达到 4 路。Datacenter Server 版是 Windows 2000 发布时最强大的服务器操作系统，可以支持 32 路 SMP 系统和 64GB 的物理内存。该系统可用于大型数据库、经济分析、科学计算以及工程模拟等方面，另外还可用于联机交易处理。

微软公司于 2003 年 3 月 28 日发布的 Windows Server 2003 是目前仍然被许多用户钟爱的服务器操作系统，主要包括下列版本：①Windows Server 2003 标准版，是针对中

小型企业服务器开发的操作系统，支持4个处理器和4G内存，可用于文件服务器、打印服务器、邮件服务器和数据库服务器等；②Windows Server 2003企业版，是针对大型企业服务器开发的操作系统，分32位版本和64位版本，其32位版本支持8个处理器、8GB内存、8个节点的群集，64位版本支持64GB内存；③Windows Server 2003数据中心版是针对大型数据仓库开发的操作系统，分32位版本和64位版本；④Windows Server 2003 Web版是针对Web服务器开发的操作系统，支持2个处理器，2GB内存，支持IIS 6.0和Internet防火墙，同时提供了对微软公司ASP. NET的支持，是构建Web服务器的理想平台。

Windows Server 2008是一套继承Windows Server 2003的服务器系统，是目前微软公司推出的使用最广泛的服务器操作系统。Windows Server 2008发行了多种版本，以支持各种规模的企业对服务器不断变化的需求。Windows Server 2008有5种不同版本，另外还有3个不支持Windows Server Hyper-V技术的版本，因此总共有8种版本。

Windows Server 2008 Standard Edition(x86 and x64)，即标准版，是迄今最稳固的Windows Server操作系统之一，其内置的强化Web和虚拟化功能是专为增加服务器基础架构的可靠性和弹性而设计的，可以有效节省时间并降低成本。

Windows Server 2008 Enterprise Edition(x86 and x64)，即企业版，其所具备的群集和热添加(Hot-Add)处理器功能可协助改善可用性，而整合的身份管理功能可协助改善安全性，利用虚拟化授权权限整合应用程序可减少基础架构的成本，提供一个企业级的平台，并部署企业关键应用。

Windows Server 2008 Datacenter Edition(x86 and x64)，即数据中心版，可支持2～64个处理器，可在小型和大型服务器上部署企业关键应用及大规模的虚拟化。其所具备的群集和动态硬件分割功能可改善可用性，而通过无限制的虚拟化许可授权来巩固应用，以建立企业级虚拟化和扩充解决方案。

Windows Web Server 2008 (x86 and x64)，即网络服务器版，是特别为单一用途Web服务器而设计的系统，而且建立在Web基础架构功能的基础上，其整合了重新设计架构的IIS 7.0、ASP. NET和Microsoft . NET Framework，以便供任何企业快速部署网页、网站、Web应用程序和Web服务。

Windows基于NT核心的系列网络操作系统具有以下特点。

(1) 内置的网络功能。通常的网络操作系统是在传统的操作系统之上附加网络软件，而Windows NT操作系统是将网络功能集成在操作系统中作为输入输出系统的一部分，在结构上更加紧凑。

(2) 可在局域网中组成异构模式，同时存在客户/服务器网络和对等式网络两种模式，各工作站可通过不同的登录方式选择不同的共享对象。

(3) 组网简单、管理方便。运用Windows NT组建网络比较简单，适合于普通用户使用。

(4) 系统设计充分考虑了企业对Internet的要求，集成网络协议标准，使其更容易与Internet连接。

(5) 新增许多与Internet密切相关的功能和服务以满足企业网的需求。

7.3 网络操作系统的选择

网络操作系统对网络的性能有着至关重要的影响，选择一个合适的网络操作系统能大大地提高系统的效率。选择网络操作系统既要分析应用系统的情况，又要分析网络操作系统的安全性与稳定性、集成性与扩展性、开放性与操作性以及价格等，还要考虑网络操作系统的技术、市场及生产厂商的变化情况。

1. 安全性与稳定性

对网络而言，安全性和稳定性的重要性是不言而喻的，网络操作系统的稳定性及可靠性将是一个网络环境得以持续高效运行的有力保证。微软公司的网络操作系统一般只用在中低档服务器中，因为其在安全性和稳定性方面较为逊色，而 UNIX 主要的特性就是安全性和稳定性高。

2. 集成性与扩展性

集成性就是对硬件及软件的容纳能力。一般构建网络都具有多种不同应用的要求，因而具有不同的硬件及软件环境，而网络操作系统作为这些不同环境集成的管理者，应有尽可能多的软硬件管理能力。

扩展性就是对现有系统进行扩充的能力。当用户应用的需求增大时，网络处理能力也要随之增加和扩展，这样可以保证用户在早期的投资不至于浪费，也为今后的发展打好基础。

NetWare 硬件适应性较差，所以其可集成性就比较差。UNIX 系统一般都是针对自己的专用服务器和工作站进行优化，其兼容性也较差。而 Linux 对 CPU 的支持比 Windows NT/2003/2008 Server 要好得多。对 TCP/IP 的支持应当是最基本的要求，对 TCP/IP 的支持程度自然也是衡量网络操作系统的一个主要指标，Windows 系列集成了 TCP/IP 协议。上述主流网络系统当然也都可以支持 TCP/IP 协议。

3. 开放性与操作性

开放性操作系统的使用，可以让第三方机构自由地开发自身适用的应用程序，良好的开发支持使第三方厂商愿意并可为其开发系统，无疑会受到用户的认可。Linux 在开放性方面具有很强的优势。

操作性是指系统要便于用户操作，实现 GUI 化操作，对硬件平台兼容性好，系统安装方便，维护难度较低，升级容易等。Windows 系列在操作性方面做得比较好。

7.4 本章小结

网络操作系统是操作系统和网络通信技术相结合的产物，不但具备操作系统的处理机管理、存储管理、设备管理和文件管理等功能，还具有网络通信、网络资源管理、网络服

务、网络管理和互操作能力。

网络操作系统的工作模式包括客户/服务器模式与对等模式两种。

常用的局域网操作系统有 Novell 公司的 NetWare 网络操作系统，微软公司的 Windows NT/2003/2008 网络操作系统，SCO 公司的 UNIX 网络操作系统，RedHat 公司的 Linux 网络操作系统等。在网络操作系统中 Linux 是与 UNIX 兼容的多用户、多任务操作系统，Linux 是自由软件，由全世界计算机爱好者们共同开发，共同使用。

微软公司推出的 Windows Server 2008 网络操作系统在性能上超越以前的版本，具有更加稳定的性能、更加安全的系统、更易操作的界面和更加强大的服务，在产品质量上占有一定的优势。网络操作系统选择既要分析应用系统的情况，又要分析网络操作系统的安全性与稳定性、集成性与扩展性、开放性与操作性以及价格等，还要考虑网络操作系统的技术、市场及生产厂商的变化情况。

综合训练

一、理论题

1. 选择题

(1) 网络操作系统是操作系统和(　　)相结合的产物。

A. 计算机系统　　B. 应用系统　　C. 网络通信技术　　D. 网络系统

(2) 网络操作系统与计算机网络内的(　　)无关，能跨越不同技术类型的网络。

A. 硬件　　B. 软件　　C. 通信　　D. 程序

(3) 一般网络操作系统的工作模式都是(　　)模式。

A. 开放　　B. C/S　　C. 共享　　D. P2P

(4) 微软公司 Windows 系列网络操作系统基于(　　)核心技术。

A. 开源　　B. TCP/IP　　C. 虚拟　　D. NT

(5) 网络操作系统(　　)的安全性与可靠性得到业界公认。

A. NetWare　　B. Linux　　C. UNIX　　D. Windows

2. 填空题

(1) 操作系统的管理功能包括________、________、________、________和________。

(2) 操作系统有________、________、________和________ 4 个主要的特性。

(3) 网络操作系统的工作模式一般有________模式和________模式。

(4) Windows Server 2003 主要包括________、________、________和________ 4 个版本。

3. 简答题

(1) 简述网络操作系统的特点。

（2）简述基于 NT 核心的 Windows 系列操作系统的特点。

（3）简述网络操作系统的选择原则。

二、实践题

1. 创建虚拟机

VMware Workstation 是一款功能强大的桌面虚拟计算机软件，能够让用户在单一的桌面上同时运行不同的操作系统，是进行开发、测试、部署新的应用程序的最佳解决方案。VMware Workstation 可在一部实体计算机上模拟完整的网络环境，是 IT 开发人员和计算机网络管理人员进行项目测试、构建实验环境的有力辅助工具。

创建虚拟机的参考步骤如下：

（1）运行 VMware Workstation 软件，如图 7-2 所示。

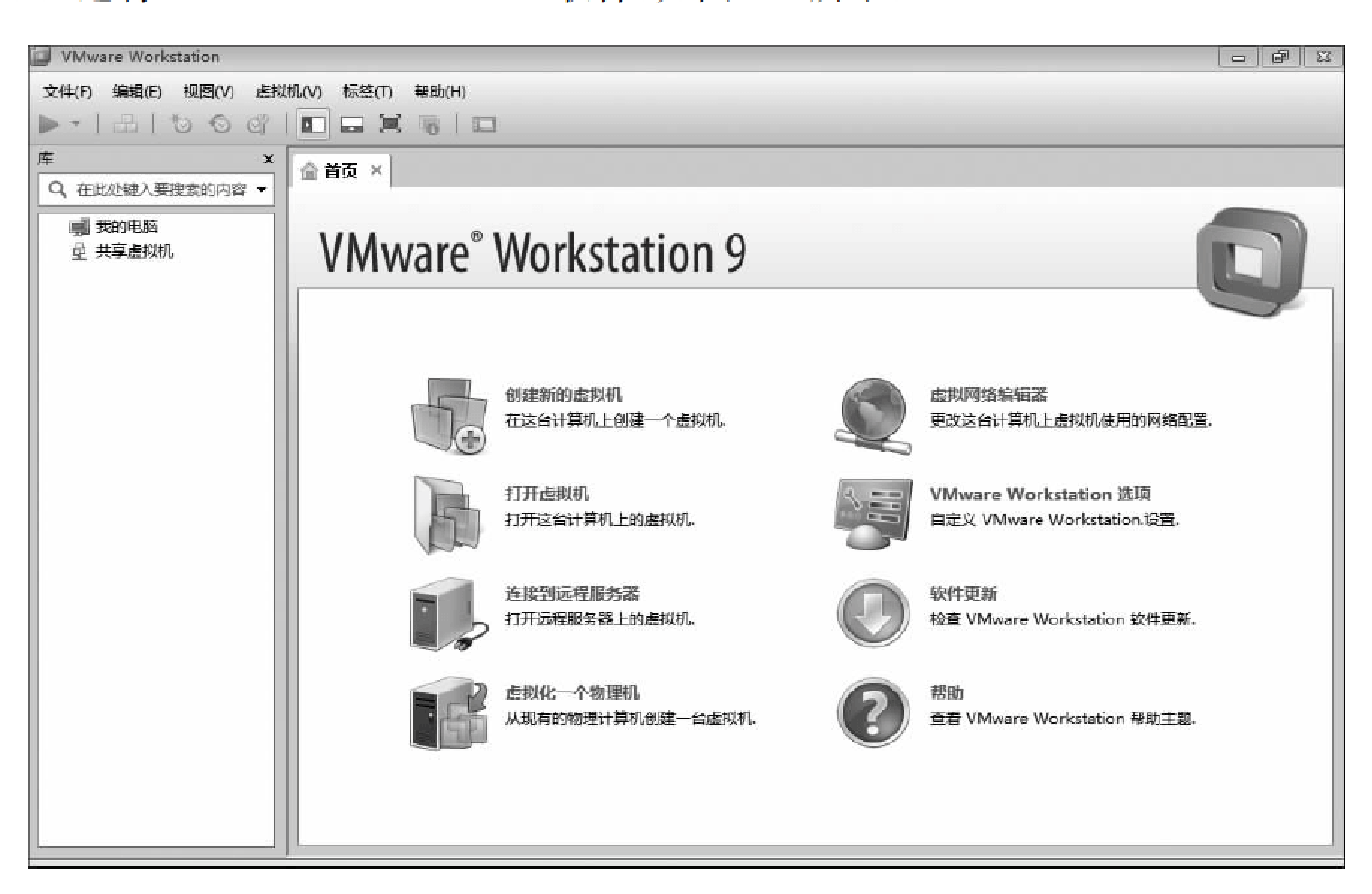


图 7-2　VMware Workstation 首页

（2）选择“创建新的虚拟机”项，出现“新建虚拟机向导”对话框，如图 7-3 所示，点选“典型”配置。

（3）确认操作系统安装盘路径，如图 7-4 所示。

（4）确定虚拟机安装操作系统的名称以及虚拟机安装的位置，如图 7-5 所示。

（5）新的虚拟机创建完成，虚拟环境如图 7-6 所示。

2. 安装 Windows Server 2008 网络操作系统

参考步骤如下：



图 7-3　“新建虚拟机向导”对话框



图 7-4　安装盘路径



图 7-5　虚拟机名称和位置

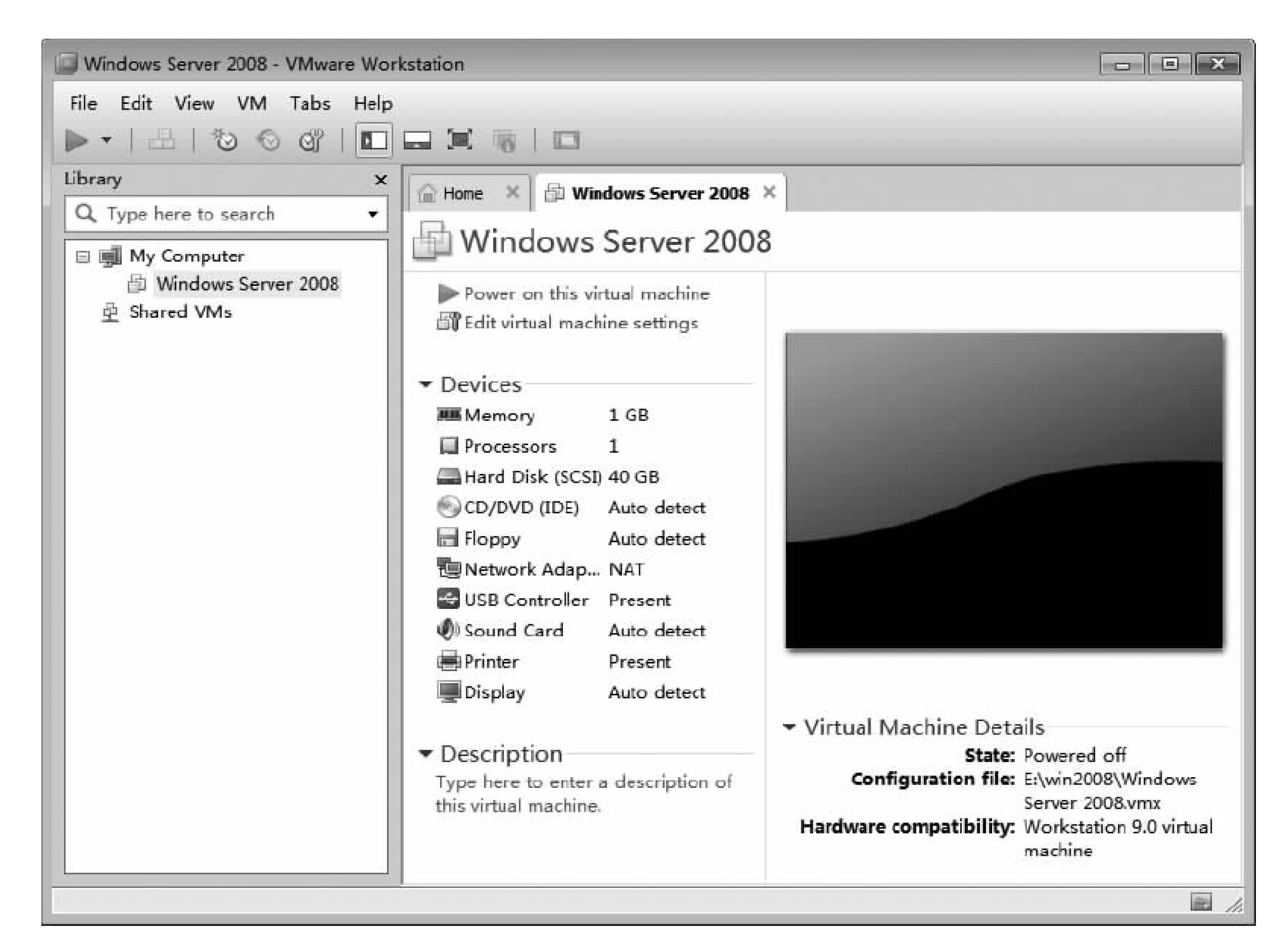


图 7-6　虚拟机环境

(1) 开始安装 Windows Server 2008，选择安装语言、时间和货币格式以及键盘和输入方法，如图 7-7 所示。



图 7-7　选择语言等首选项

(2)选择操作系统版本，如图7-8所示。



图7-8 版本选择

(3)选择安装方式，如图7-9所示。



图7-9 安装方式

（4）选择安装路径，如图 7-10 所示。



图 7-10 选择安装路径

（5）安装自动进行，如图 7-11 所示。

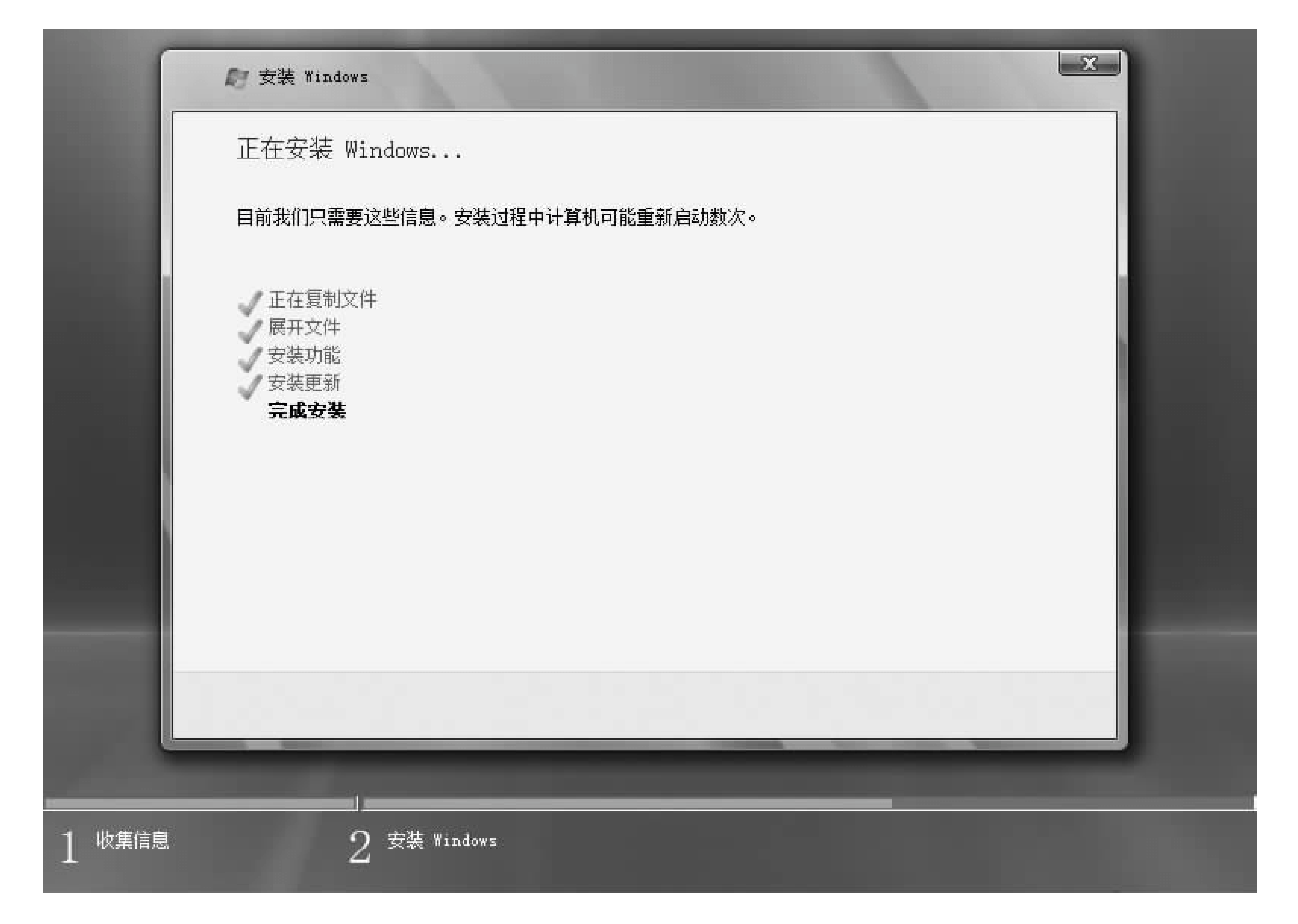


图 7-11 安装进行中

（6）操作系统安装结束，如图 7-12 所示。



图 7-12　安装结束

第 8 章　Windows Server 2008 服务器配置与管理

本章主要内容

- IIS
- Web 服务器配置与管理
- FTP 服务器配置与管理
- DNS 服务器配置与管理
- DHCP 服务器配置与管理
- 邮件服务器配置与管理

网络操作系统的主要功能是为计算机网络提供服务。Windows Server 2008 操作系统具有强大的网络服务功能，如 WWW 服务、FTP 服务、DNS 服务和 DHCP 服务等。IIS 是一套集成的服务器服务，用以支持 HTTP、FTP 和 SMTP，它能够提供快速集成产品，同时可扩展 Internet 服务器。

8.1　IIS

8.1.1　IIS 的功能

IIS 是 Internet Information Service 的缩写，即因特网信息服务，它是微软公司的网络操作系统的重要服务，IIS 与 Window NT Server 完全集成在一起，因而用户能够利用 Windows NT Server 和 NTFS(NT File System，NT 文件系统)内置的安全特性，建立强大、灵活而安全的 Internet 及 Intranet 站点。IIS 支持 HTTP(Hypertext Transfer Protocol，超文本传输协议)，FTP(File Transfer Protocol，文件传输协议)以及 SMTP(Simple Mail Transfer Protocol，简单邮件传输协议)等协议。

Windows Server 2008 操作系统集成了 IIS 7.0，通过该服务可以搭建 Web 网站，通过 Internet 及 Intranet 实现用户共享信息。IIS 7.0 是一个集成了 IIS、ASP.NET 和 Windows Communication Foundation 的 Web 统一平台，可以运行当前流行的具有动态交互功能的 ASP.NET 网页，支持使用任何与.NET 兼容的语言编写的 Web 应用程序。

IIS 7.0 提供了基于任务的全新 UI(用户界面)，并新增了功能强大的命令行工具，借助这些工具可以方便地实现对 IIS 和 Web 站点的管理。同时，IIS 7.0 引入了新的配置存储、故障诊断和排除功能。

默认情况下，在安装 Windows Server 2008 时不会自动安装 IIS。

8.1.2 IIS 的安装

(1) 启动 Windows Server 2008 时，系统默认会启动“初始配置任务”窗口，如图 8-1 所示。也可以通过选择“开始”→“管理工具”→“服务器管理器”打开服务器管理器窗口。



图 8-1　初始配置任务窗口

(2) 选择“添加角色”，打开“添加角色向导”的第一步“选择服务器角色”窗口，选择“Web 服务器(IIS)”复选框，如图 8-2 所示。

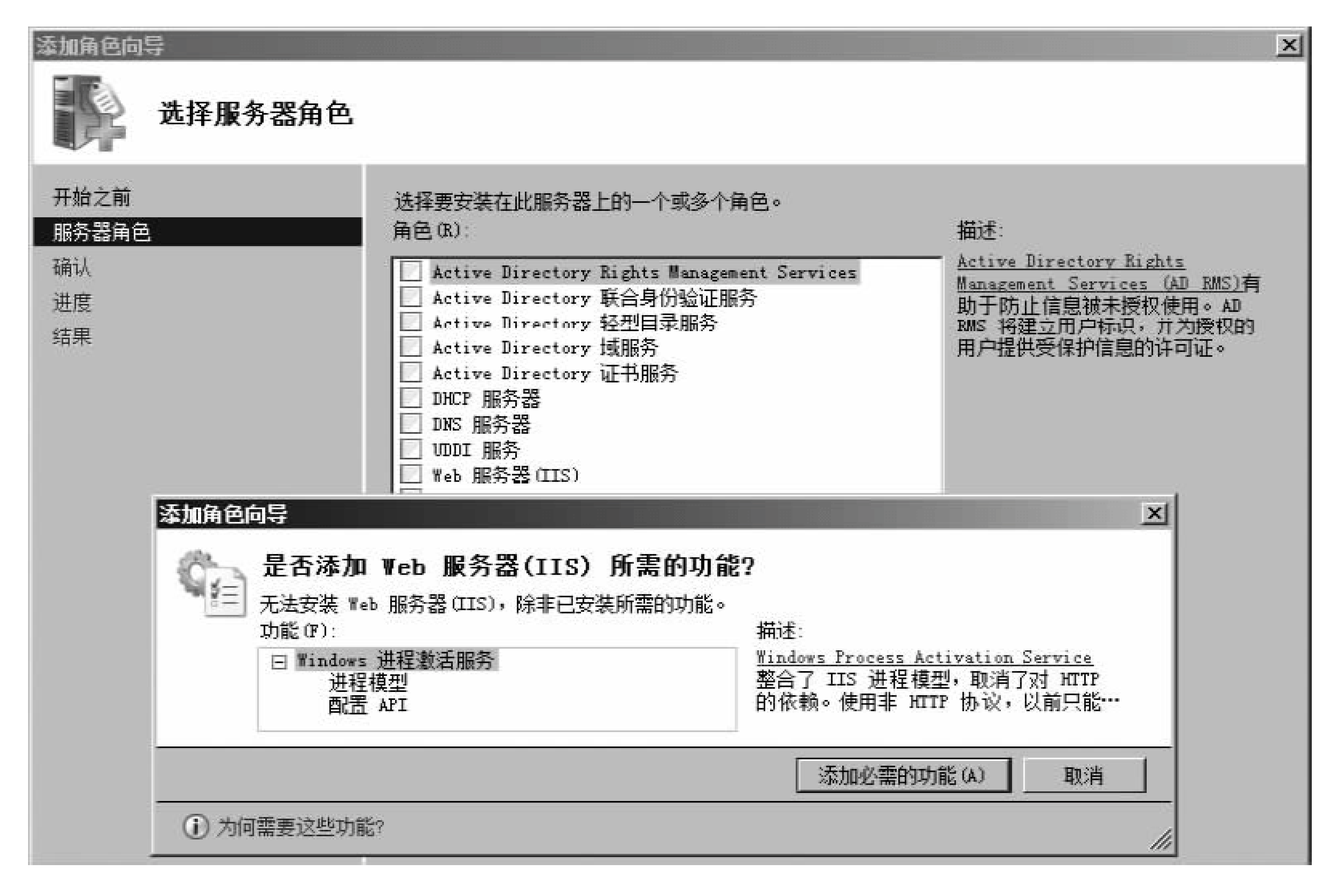


图 8-2　选择服务器角色

(3) 在“添加角色向导”对话框中，单击“添加必需的功能”按钮，选定“Web 服务器(IIS)”，窗口右侧会列出 Web 服务器的简要介绍及注意事项，如图 8-3 所示。

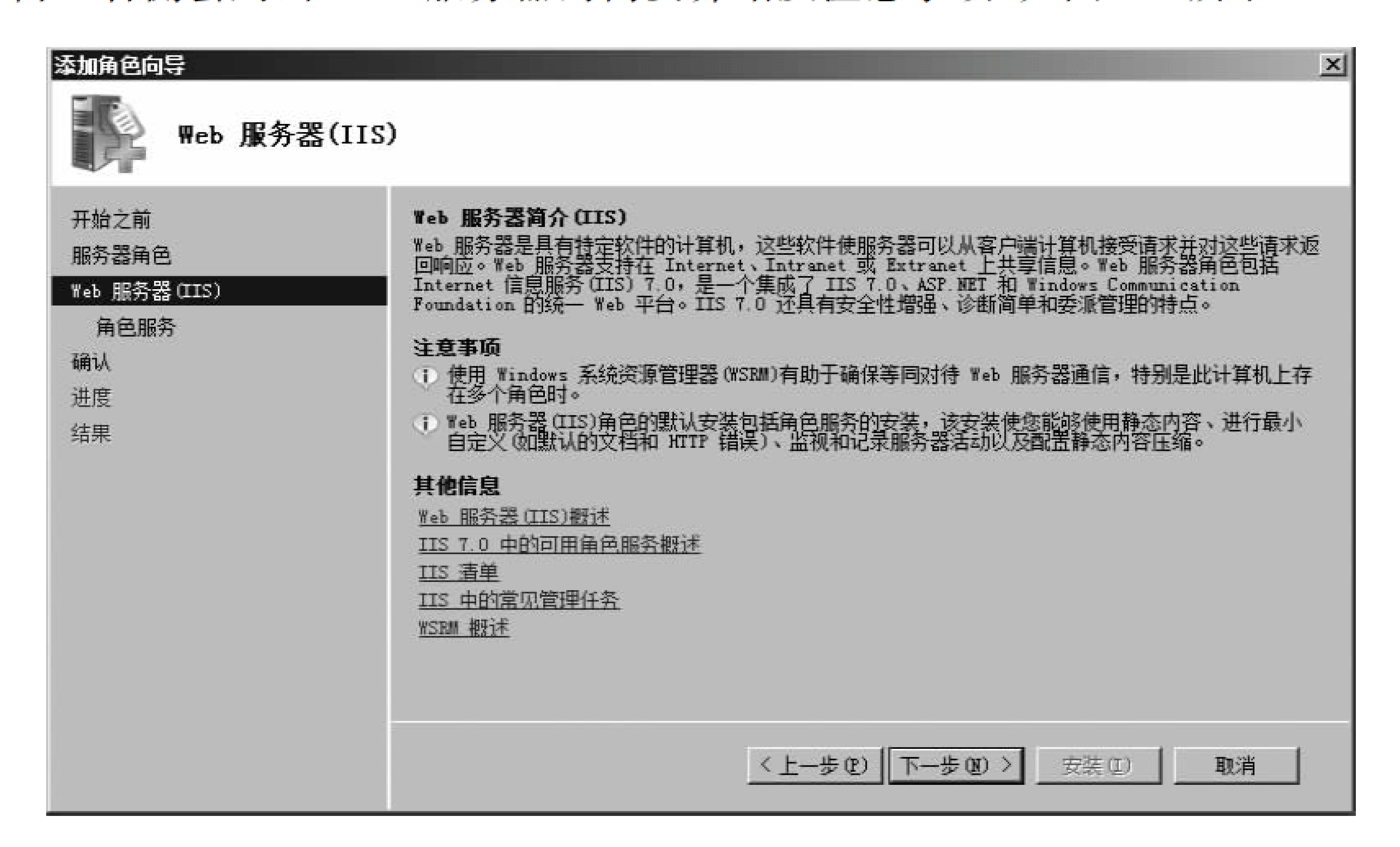


图 8-3 Web 服务器(IIS)

(4) 单击“下一步”按钮，在“选择角色服务”对话框中列出了 Web 服务器所包含的所有组件，用户可以对服务项进行选择。需要注意的是，在“应用程序开发”角色服务选项中，用户需要根据 Web 应用程序开发技术进行相应选择，如图 8-4 所示。

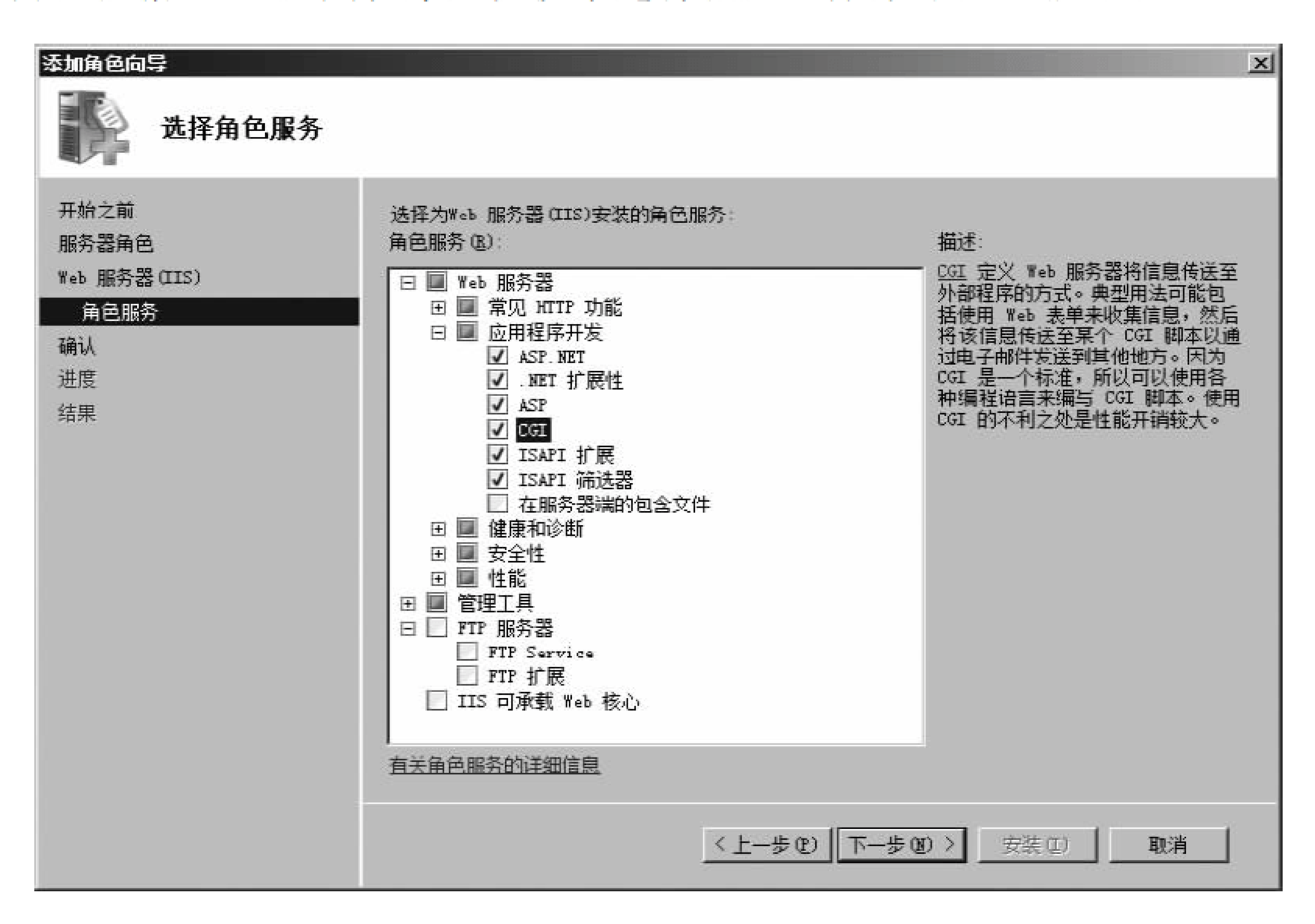


图 8-4 选择角色服务

(5) 单击“下一步”按钮，显示“确认安装选择”对话框，列出了前面选择的角色服务和功能，供用户核对，如图 8-5 所示。

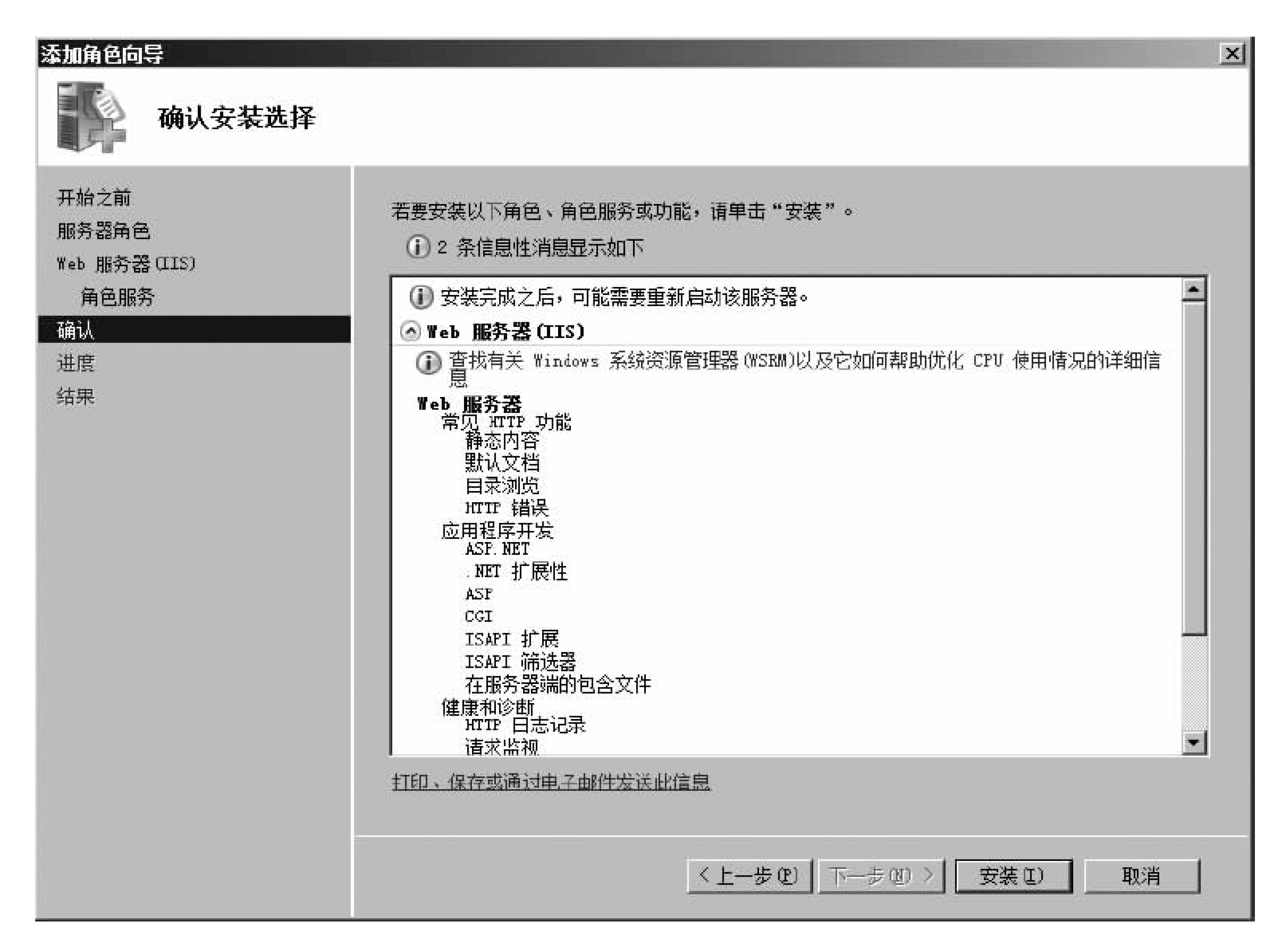


图 8-5　确认安装选择

(6) 单击“安装”按钮，即可开始安装 Web 服务器。Web 服务器安装完成后，打开“Internet 信息服务(IIS)管理器”窗口，在已安装的 Web 服务器中已经创建了 Default Web Site 的默认站点，如图 8-6 所示。



图 8-6　Internet 信息服务(IIS)管理器

(7) 验证 IIS 服务器。打开浏览器，在地址栏输入 http://localhost 或者 Http://本机 IP 地址，如果出现如图 8-7 所示的页面，说明 Web 服务器(IIS)安装成功；否则，说明

Web 服务器安装失败，需要重新检查服务器设置或者重新安装。

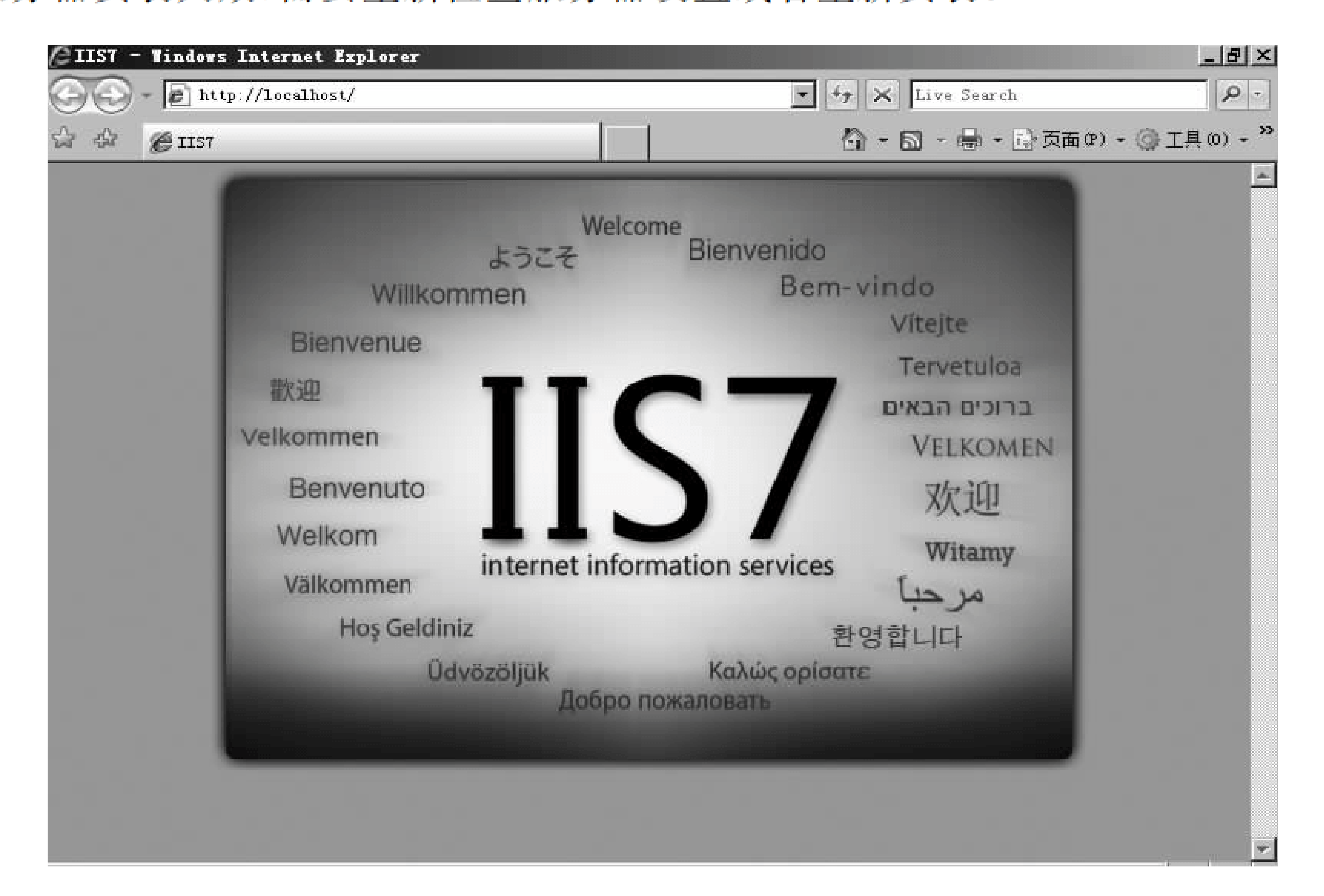


图 8-7　Web 服务器欢迎页面

到此，Web 服务器(IIS)就安装完成了，随后就可以进行站点发布。用户可以将做好的网页文件放到 C:\inetpub\wwwroot 文件夹，然后在浏览器地址栏输入 http://localhost 或者 http://本机 IP 地址浏览网页。

8.2　Web 服务器新建站点配置与管理

8.2.1　Web 服务及其工作原理

万维网(World Wide Web，WWW)是一种建立在 Internet 上的全球性的、交互的、动态多平台的分布式信息系统。它允许用户在一台计算机上通过 Internet 访问另一台计算机上的信息。其特点为：以超文本方式组织网络多媒体信息；可以在世界范围内任意查找、检索、浏览及添加信息；提供生动直观、易于使用、统一的图形用户界面；Web 站点之间可以互相链接，可以提供信息查找和漫游的透明访问；可访问图像、声音、视频与文本信息。

WWW 服务工作原理如图 8-8 所示，WWW 服务采用客户/服务器工作模式。客户端的应用程序是 Web 浏览器，服务器端则安装提供 WWW 服务的软件，它们以超文本标记语言(HTML)与超文本传输协议(HTTP)为基础，为用户提供界面一致的信息浏览。

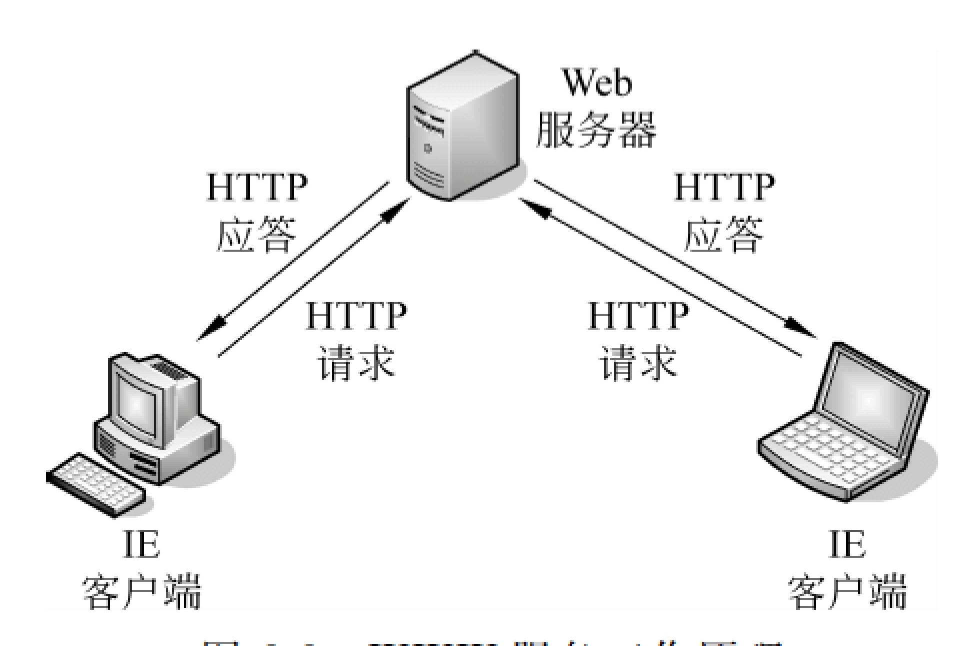


图 8-8　WWW 服务工作原理

8.2.2 新建站点安装配置

Web 服务器安装好之后，会创建一个 Defalut Web Site 的默认站点，使用该站点就可以创建网站。但是，在实际工作中，用户开发网站时会在 Web 服务器中新建站点，以方便管理自己的网站文件，下面介绍新建站点安装配置。

例 8-1 发布一个名为 sunline 的站点，主目录为 C:\sunline，网站主页为 Happy.htm。

(1) 选择“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”，在窗口中右击“网站”，在快捷菜单中选择“添加网站”命令，打开“添加网站”对话框，如图 8-9 所示。



图 8-9 “Internet 信息服务(IIS)管理器”窗口

(2) 在“添加网站”对话框中添加新建网站名称、物理路径以及 Web 站点需要绑定的计算机 IP 地址与端口信息。一般情况下，一个网站只能对应一个 IP 地址，默认端口为 80，主机名借助 DNS 服务可以实现通过域名访问网站，如图 8-10 所示。

Web 服务器默认的端口是 80 端口，如果设置的端口不是 80，比如是 8000，那么访问 Web 服务器就需要在地址栏输入 http://192.168.1.111:8000。

(3) 新建网站添加完成，如图 8-11 所示。

(4) 配置站点主目录。站点主目录即网站的根目录，保存着 Web 网站的相关资源。默认站点 Defalut Web Site 的默认路径为 C:\Inetpub\wwwroot 文件夹。用户可以根据需要更改网站的主目录，即“物理路径”，例如 C:\sunline。打开 IIS 管理器，选择 Web 站点，单击右侧“操作”栏中的“基本设置”超级链接，如图 8-12 所示。

(5) 配置默认文档，即访问网站的主页。通常，Web 网站的主页都会设置成默认文档，当用户使用 IP 地址或者域名访问时，就不需要再输入主页名，从而便于用户的访问。

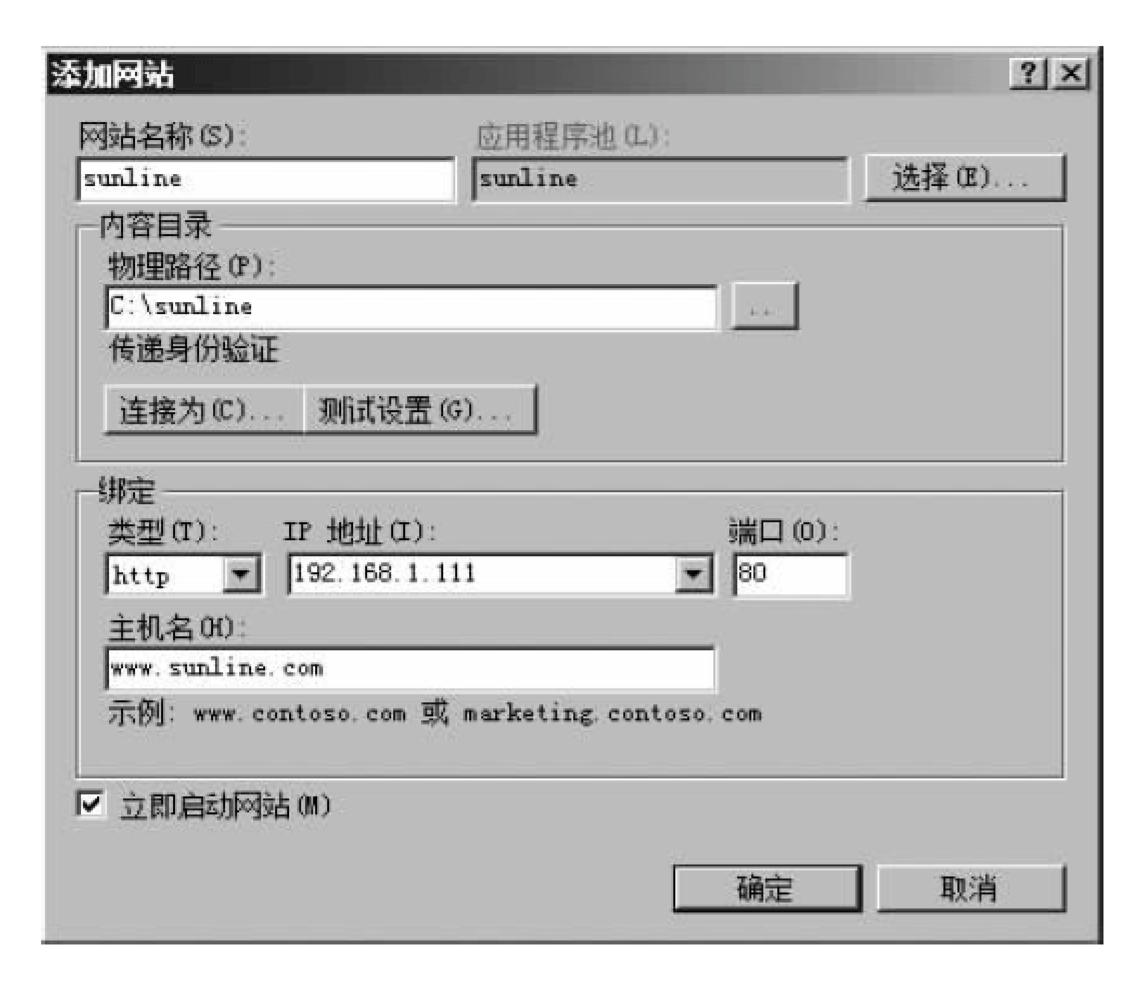


图 8-10 “添加网站”对话框



图 8-11 新建站点添加完成

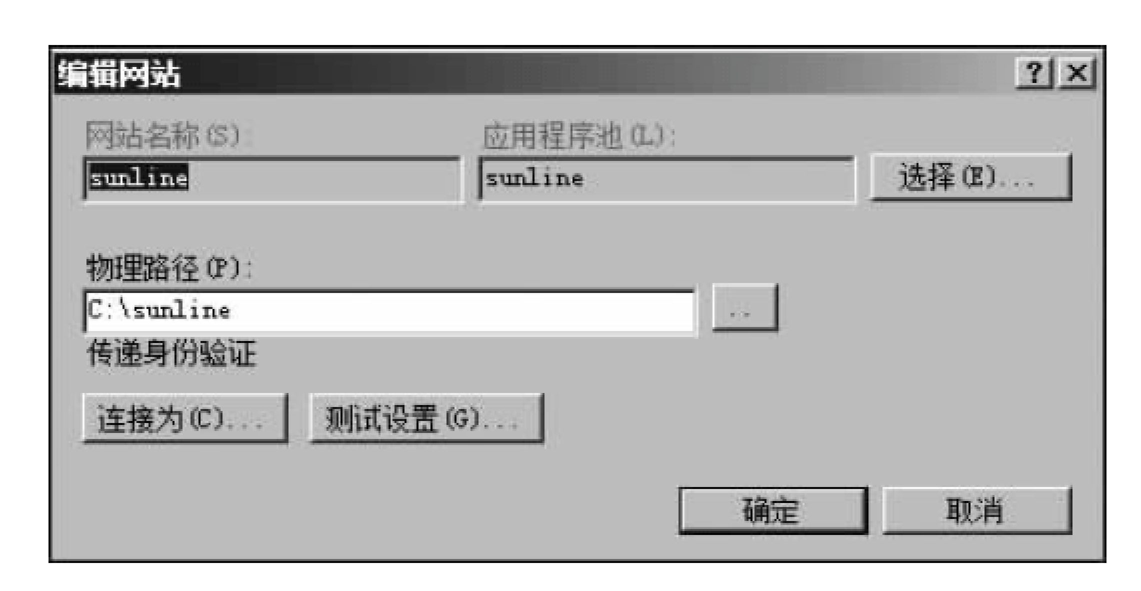


图 8-12 “编辑网站”对话框

在 IIS 管理器中选择 Web 站点，在“sunline 主页”窗口中双击“IIS”区域的“默认文档”图标，如图 8-13 所示。

系统有 6 种默认文档，如果要使用其他名称的默认文档，例如，当前 sunline 网站主页

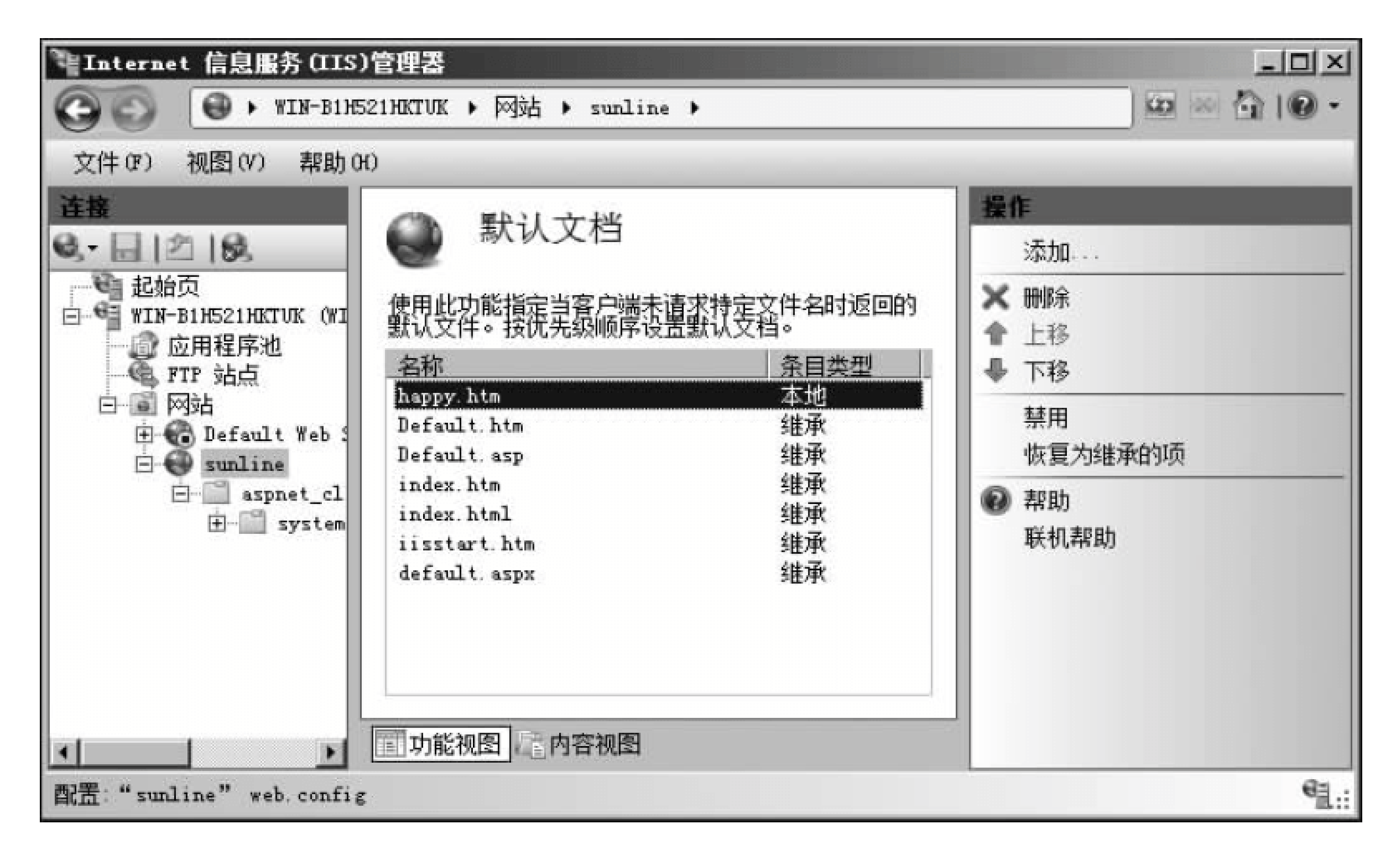


图 8-13 默认文档设置窗口

为 happy.htm，则需要添加该名称为默认文档。单击右侧的"添加"超链接，显示如图 8-14 所示的窗口，在"名称"文本框中输入要使用的主页名称。单击"确定"按钮，即可添加该默认文档。新添加的默认文档自动排在最上面。

(6) 配置访问限制。选中 sunline 站点，单击右侧"操作"栏中的"限制"超链接，打开"编辑网站限制"对话框。IIS 7.0 中提供了两种限制连接的方法，分别为限制带宽使用和限制连接数，如图 8-15 所示。



图 8-14 添加默认文档

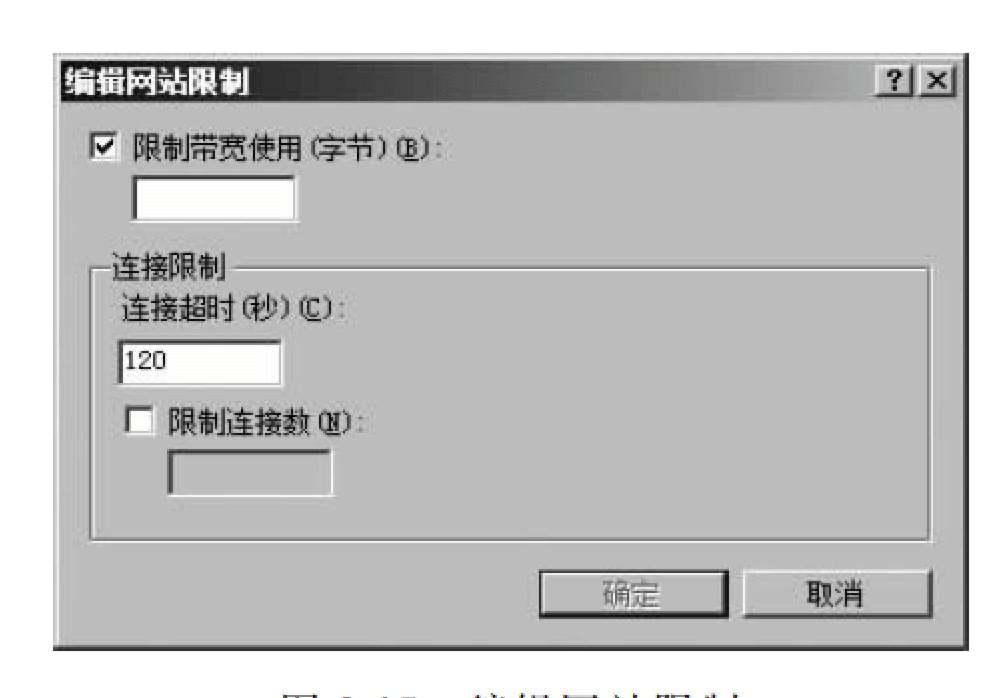


图 8-15 编辑网站限制

Web 服务器是供用户访问的，因此，不管使用的网络带宽有多充裕，都有可能因为同时连接的计算机数量过多而使服务器死机。所以有时候需要对网站进行一定的限制，例如，限制带宽和连接数量等。

选择"限制带宽使用(字节)"复选框，在文本框中输入允许使用的最大带宽值。在控制 Web 服务器向用户开放的网络带宽值的同时，也可能降低服务器的响应速度。但是，当用户 Web 服务器的请求增多时，如果通信带宽超出了设定值，请求就会被延迟。

选择"限制连接数"复选框，在文本框中输入限制网站的同时连接数。如果连接数量

达到指定的最大值，以后所有的连接尝试都会返回一个错误信息，连接将被断开。限制连接数可以有效防止试图用大量客户端请求造成 Web 服务器负载的恶意攻击。在“连接超时”文本框中输入超时时间，可以在用户端达到该时间时，显示为连接服务器超时等信息，默认是 120s。

(7) 在客户端浏览器中输入 Web 服务器地址 192.168.1.111，测试新建站点的配置结果，如图 8-16 所示。



图 8-16　新建站点测试

8.3　FTP 服务器配置与管理

8.3.1　文件服务与资源共享

FTP (File Transfer Protocol，文本传输协议)是 Internet 提供的基本服务之一。在 TCP/IP 协议体系结构中位于应用层。

FTP 指通过 Internet 将文件从一台计算机传送到另一台计算机，即文件传输。不管这两台计算机相距多远，也不管什么样的硬件，安装什么操作系统，只要连入 Internet，FTP 都能够实现 Internet 上两站之间的文件传输与复制。文件传输使用的是文件传输协议(FTP)，用于文件的上传和下载。“上传”文件指将用户计算机中的文件复制到远程服务器上，“下载”文件指将远程服务器上的文件复制到用户计算机中。

FTP 是一种实时联机服务，它采用客户/服务器结构，在进行 FTP 操作时，既需要客户应用程序，也需要服务器应用软件。

8.3.2　FTP 服务器安装配置

Windows 网络操作系统和 IIS 信息服务系统中具有 FTP 服务功能，但由于其在实际应用中存在不足之处，出现了更加方便实用的 FTP 应用软件。FTP 应用软件种类繁多，下面介绍一款适合个人计算机用户使用的 FTP 软件，即 Serv-U FTP 软件。

（1）运行 Serv-U 安装程序，如图 8-17 所示。



图 8-17　安装 Serv-U

（2）确定 Serv-U 软件安装路径，如图 8-18 所示。



图 8-18　确定安装路径

（3）运行 Serv-U 软件，如图 8-19 所示。

（4）首次运行软件时要创建域，即添加 FTP 服务器作用域，如 sun，如图 8-20 所示。也可以在以后使用中添加域，如图 8-20 所示。

（5）确定 FTP 服务涉及的协议端口，一般采用默认端口即可，通常 FTP 端口号为 21，如图 8-21 所示。



图 8-19 Serv-U 主页







图 8-20 域名设置　　　　图 8-21 协议端口设置

(6) 确定 FTP 服务器的 IP 地址，如 192.168.1.112，如图 8-22 所示。

(7) 确定 FTP 服务器用户密码的加密方式，通常使用“使用服务器设置”加密方式，如图 8-23 所示。

(8) Serv-U FTP 服务器第一个域设置完成，如图 8-24 所示。

(9) 打开域的设置用户向导，为域配置用户信息，如 sun001，如图 8-25 所示。

(10) 设置用户密码，如 123456，如图 8-26 所示。



图 8-22 IP 地址设置

图 8-23 用户加密方式选择

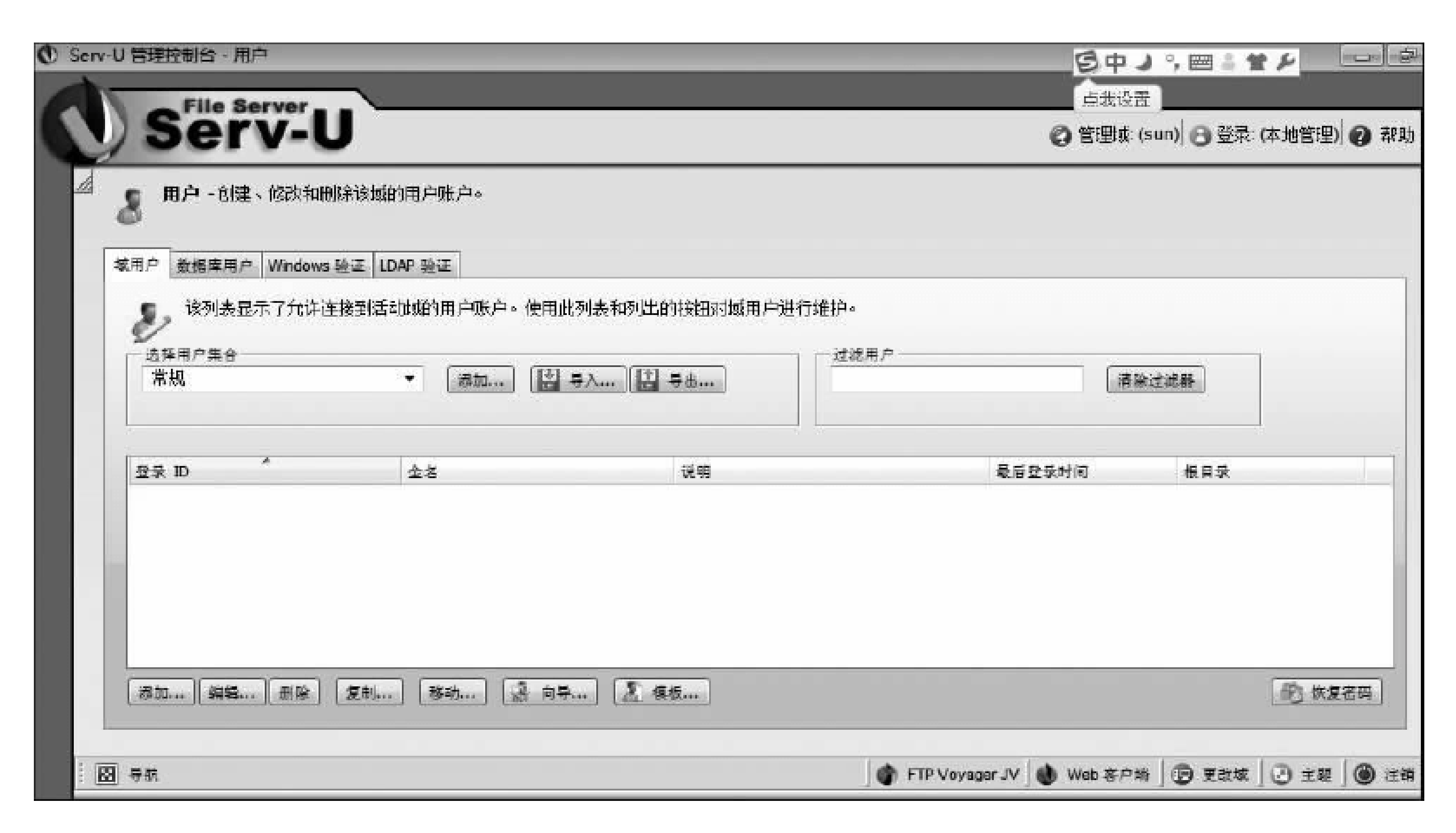


图 8-24 域设置完成

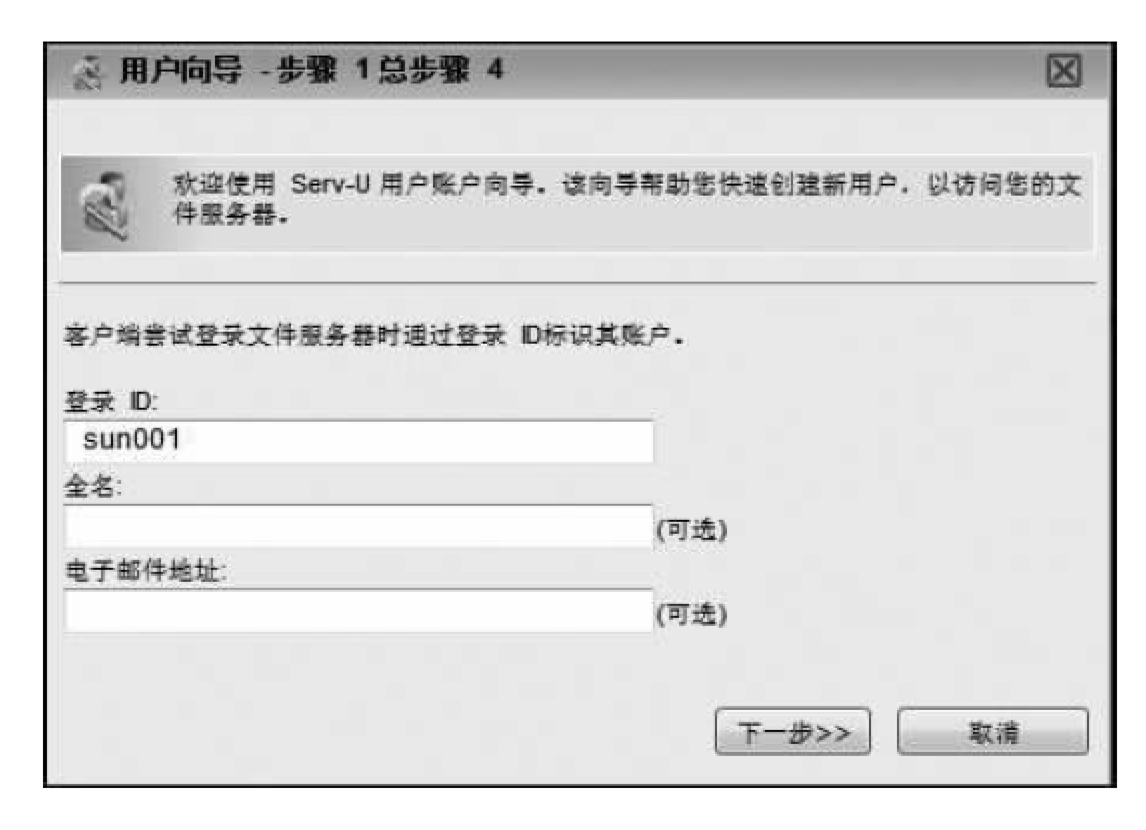


图 8-25 配置用户信息

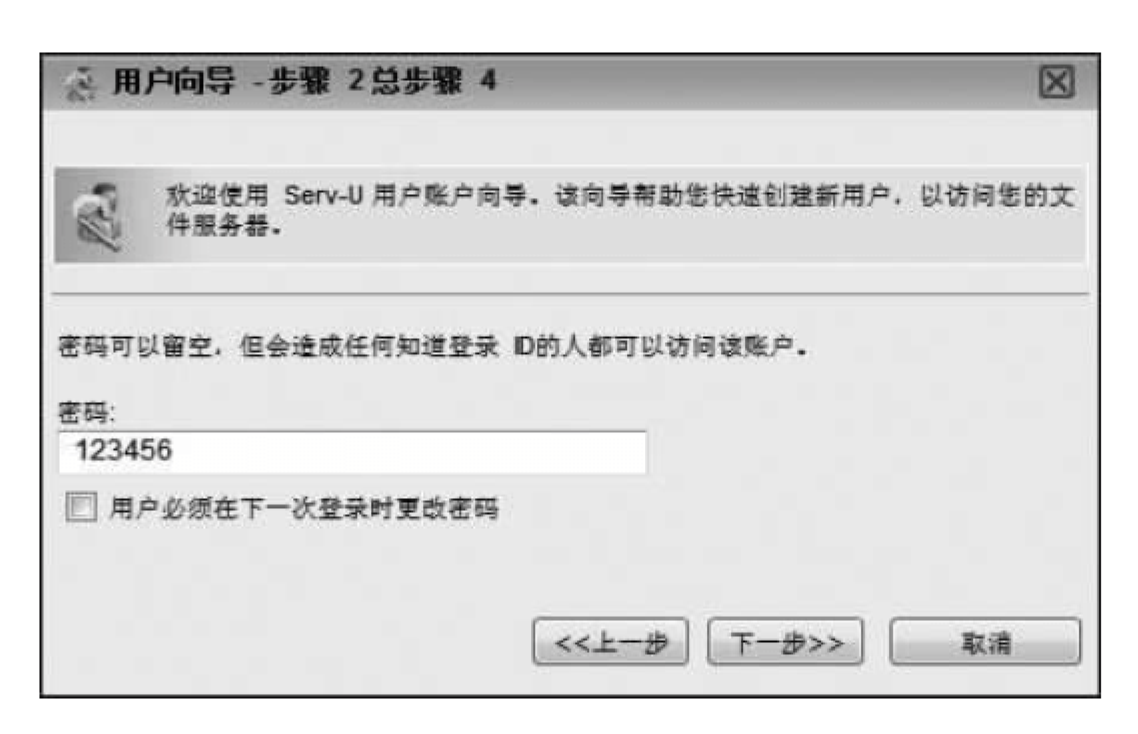


图 8-26　设置用户密码

(11) 指定用户访问路径，如 D:/sunline，如图 8-27 所示。

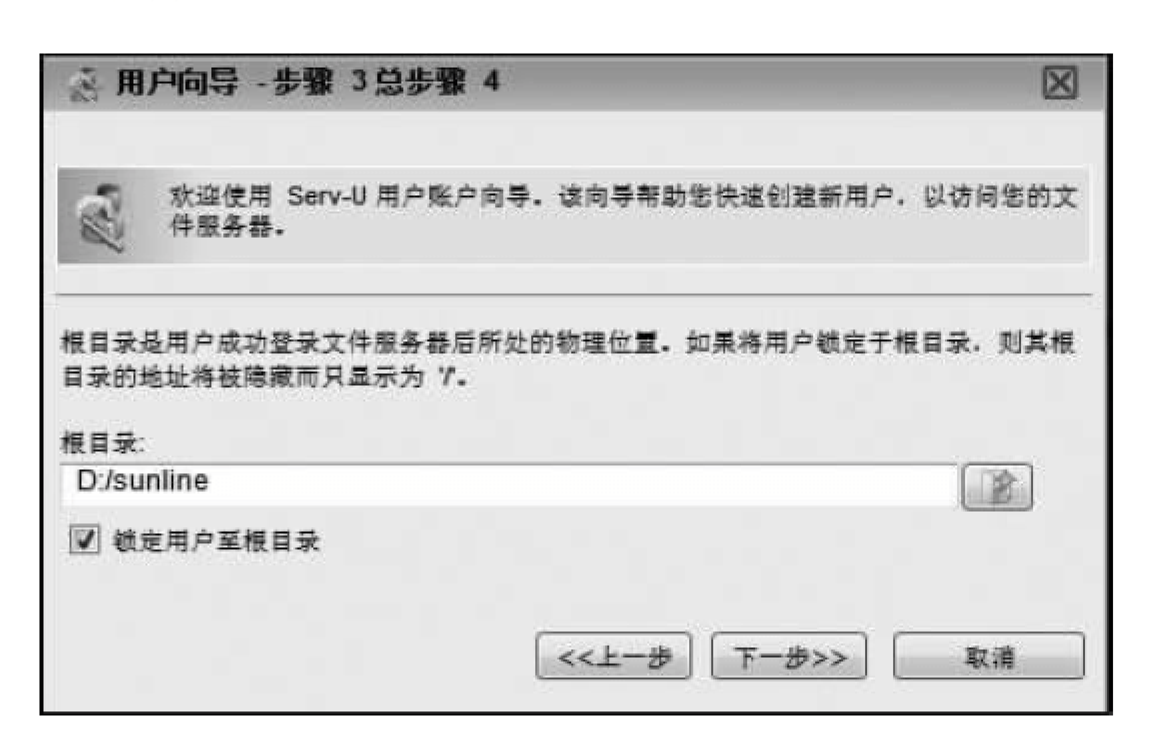


图 8-27　访问路径

(12) 设置用户访问 FTP 服务器的权限，“只读访问”是指用户只能读(即下载)FTP 服务器信息，“完全访问”指用户具有包括读/写(即下载与上传)在内的 FTP 服务器访问权限，如图 8-28 所示。

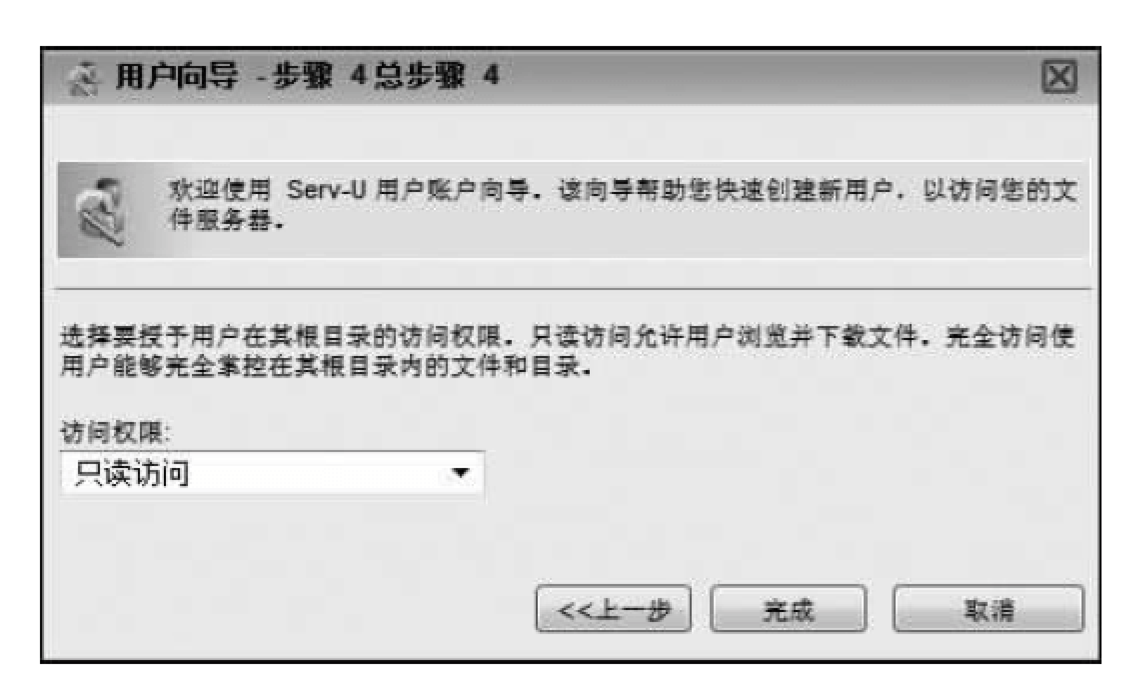


图 8-28　访问权限

(13) Serv-U FTP 服务器设置完成，如图 8-29 所示。

(14) 从客户端访问 FTP 服务器。在浏览器地址栏中输入服务器地址，如 ftp://

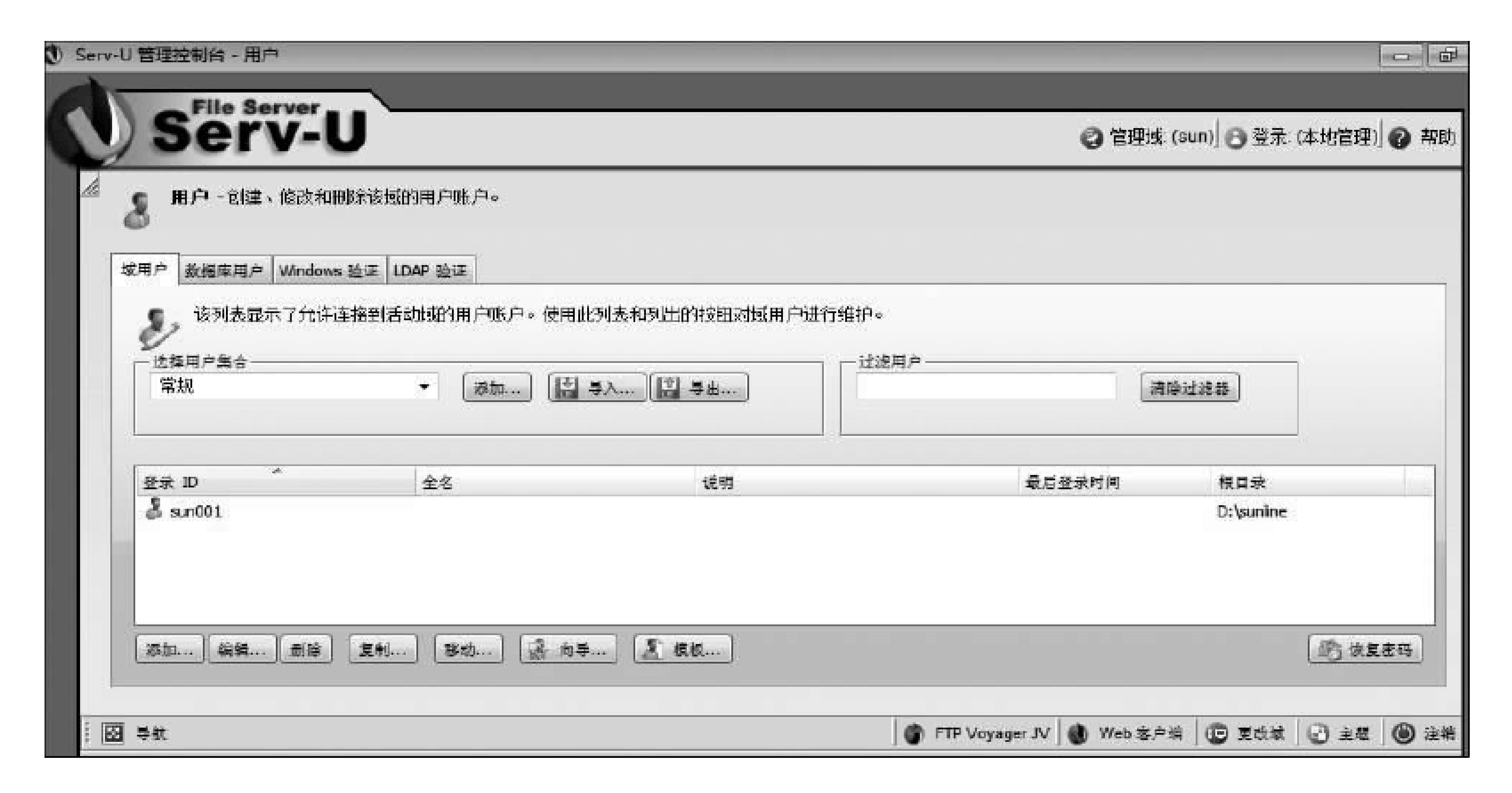


图 8-29　服务器设置完成

192.168.1.112，在弹出的对话框中输入用户名及密码，如 sun001/123456，如图 8-30 所示。



图 8-30　客户端测试

（15）根据需要，可以添加不同权限的用户与服务器。

8.4　DNS 服务器配置与管理

8.4.1　DNS 及其工作原理

DNS(Domain Name Service，域名服务)是计算机域名系统的缩写，它是由解析器以及域名服务器组成的。域名服务器是指保存有作用域网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。在 IPv4 中，IP 是由 32 位二进制数组成的，将这 32 位二进制数分成 4 组，每组 8 位二进制数，将这 8 位二进制数转化成十进制数，就是我们看到的 IP 地址。DNS 能够使用户更方便地访问互联网，而不用去记住能够被计算机直接读取的 IP 地址。

域名采用层次结构，每层构成独立的子域，层次子域之间采用圆点隔开，格式如下：

主机名域.组织名称域.组织类别域.国家地区域

例如，www.tsinghua.edu.cn 表示万维网.清华大学.学校.中国。

组织类别域与国家地区域如表 8-1 所示。

表 8-1　组织类别域与国家地区域

组织类别域		国家地区域(举例)	
com	商业，企业	ar	阿根廷
edu	学校，教育部门	au	澳大利亚
gov	政府部门	br	巴西
int	国际组织	ca	加拿大
mil	军事组织	cn	中国
net	网络中心	us	美国
org	非营利组织	tw	中国台湾

8.4.2　DNS 服务器安装配置

例 8-2　发布本地计算机 C:\sunline 站点信息，服务器 IP 地址为 192.168.1.111，访问域名为 www.sunline.com。

(1) 选择“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口，添加服务器角色，如图 8-31 所示。



图 8-31　添加服务器角色

(2) 在"添加角色向导"对话框中,勾选"DNS 服务器"复选框,如图 8-32 所示。



图 8-32　选择服务器角色

(3) 单击"下一步"按钮,在"DNS 服务器"中列出了 DNS 服务器简介与注意事项等信息,如图 8-33 所示。



图 8-33　DNS 服务器简介

(4) 确认 DNS 服务器的安装选择,如图 8-34 所示。

至此,DNS 服务器安装成功,如图 8-35 所示。但要提供域名解析服务,还必须进行下列设置。

(5) 开始设置 DNS 服务器。选择"开始"→"管理工具"→DNS 选项,打开 DNS 管理器,如图 8-36 所示。



图 8-34 确认安装选择

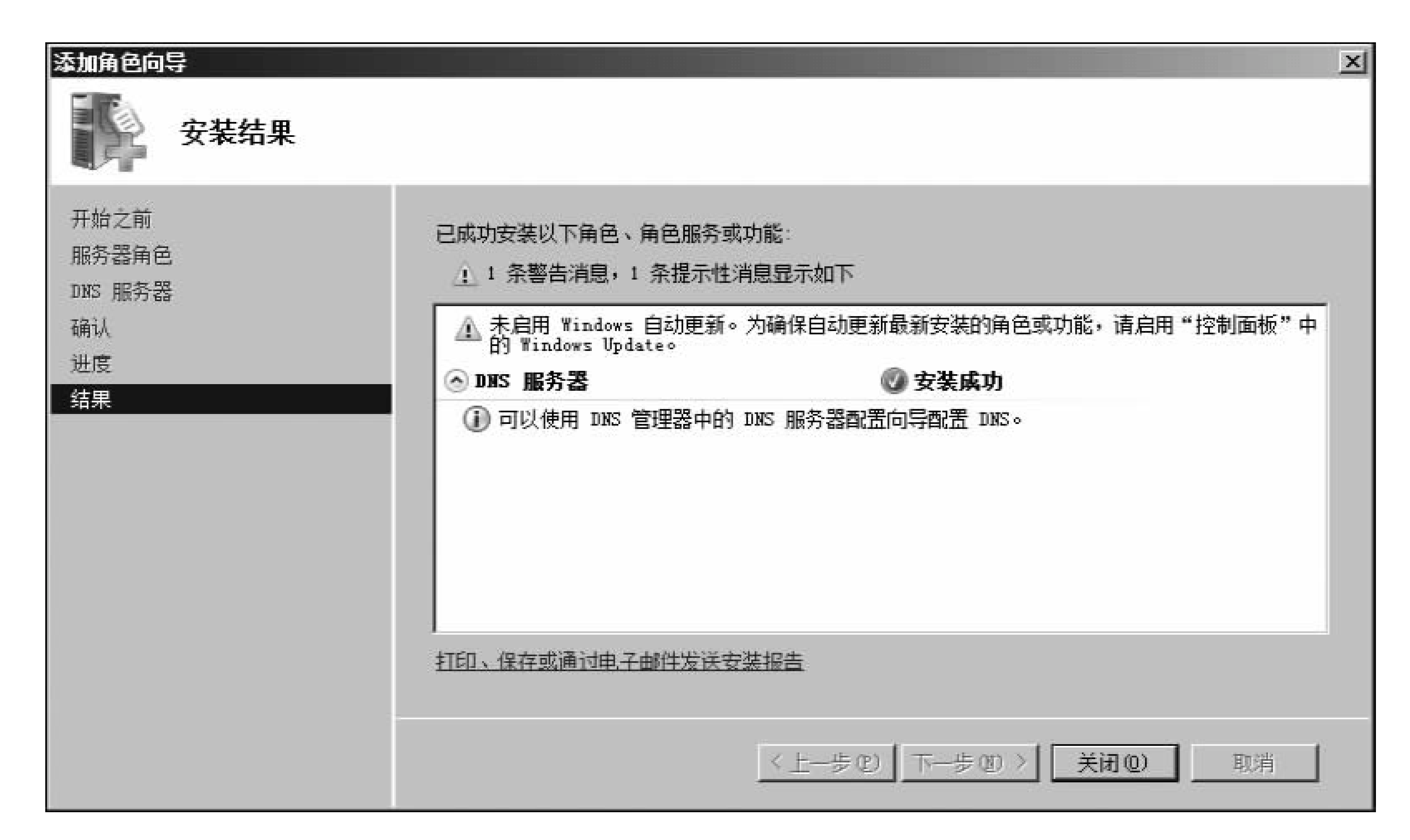


图 8-35 DNS 服务器安装成功

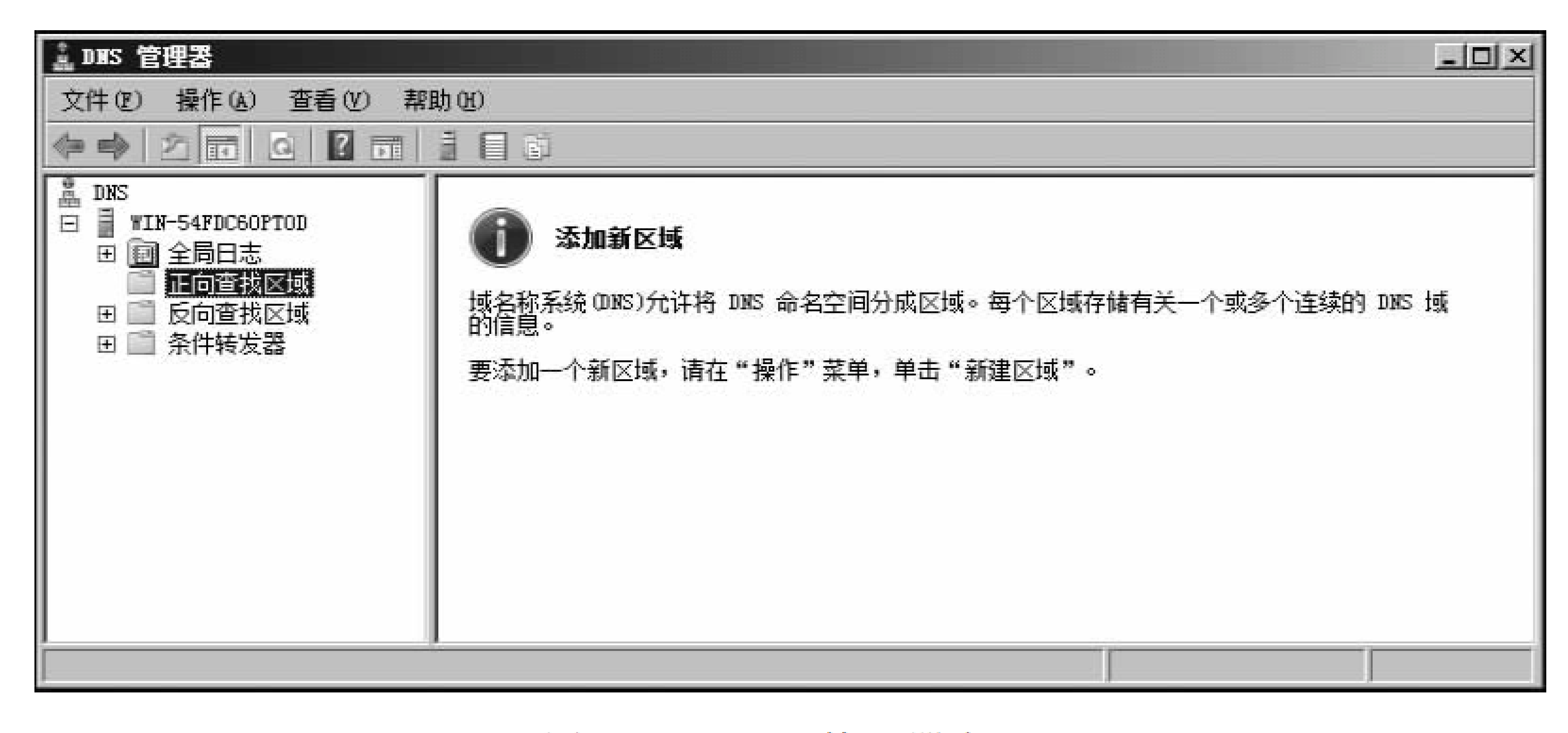


图 8-36 DNS 管理器窗口

（6）为了使 DNS 服务器能够将域名解析成 IP 地址，首先在 DNS 区域中添加正向查找区域，如图 8-37 所示。

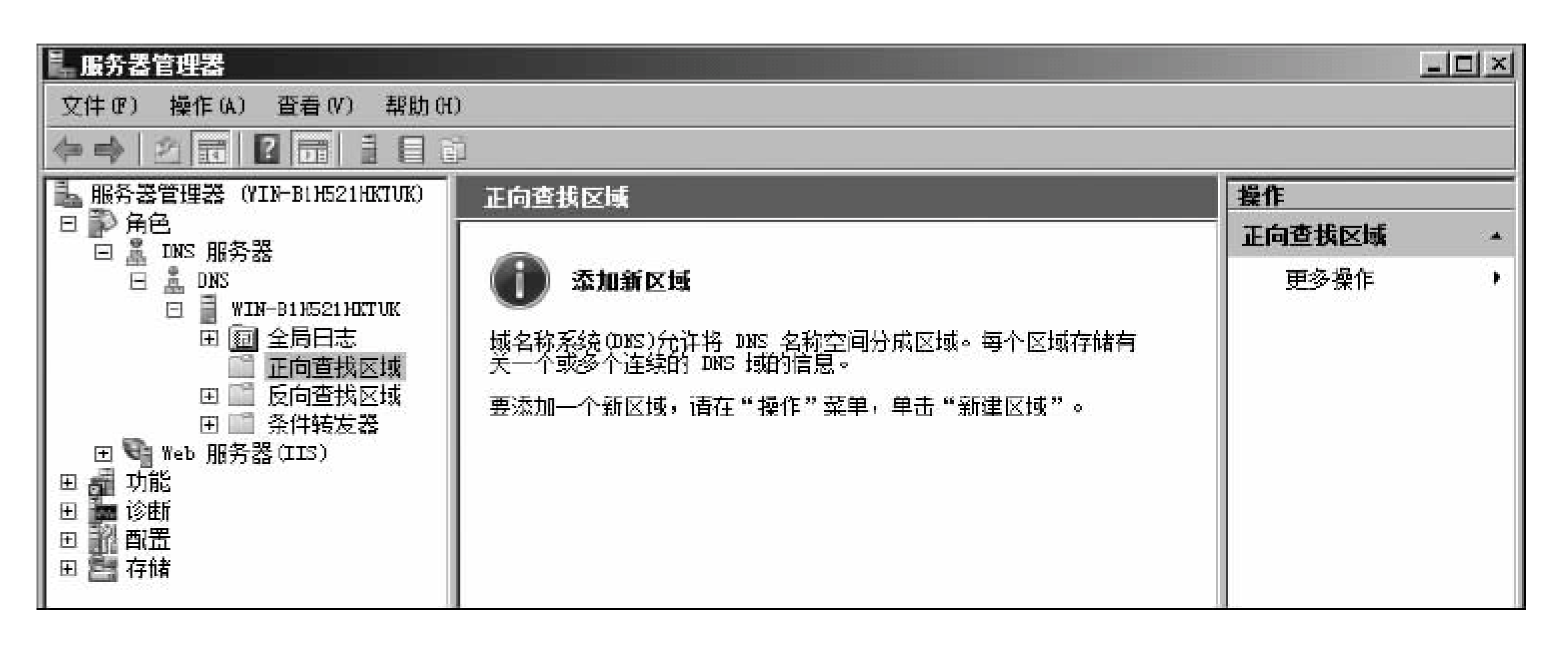


图 8-37　添加正向查找区域

（7）右击“正向查找区域”，在快捷菜单中选择“新建区域”命令进入“新建区域向导”对话框，如图 8-38 所示。



图 8-38　新建区域向导

（8）在“新建区域向导”的“区域类型”对话框中，选择“主要区域”单选按钮，如图 8-39 所示。

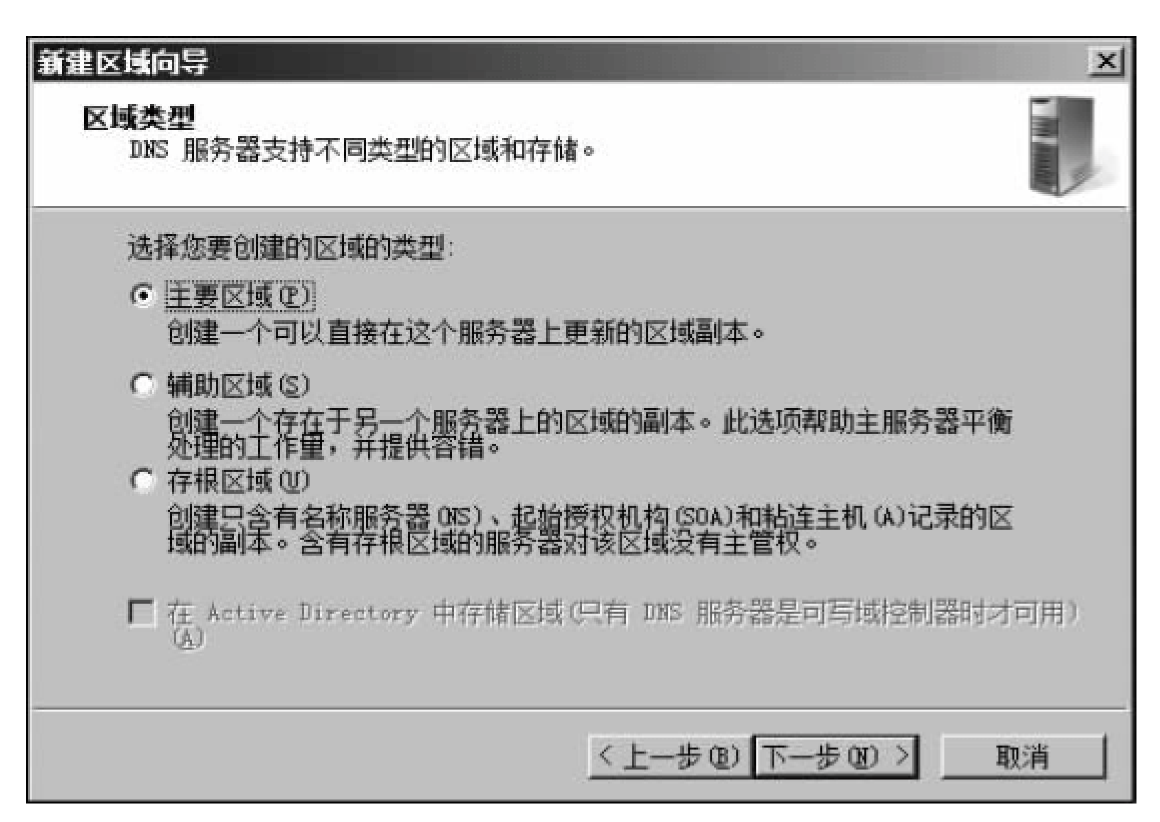


图 8-39　选择区域类型

（9）在“新建区域向导”的“区域名称”对话框中，添加区域名称：sunline.com，如图 8-40 所示。

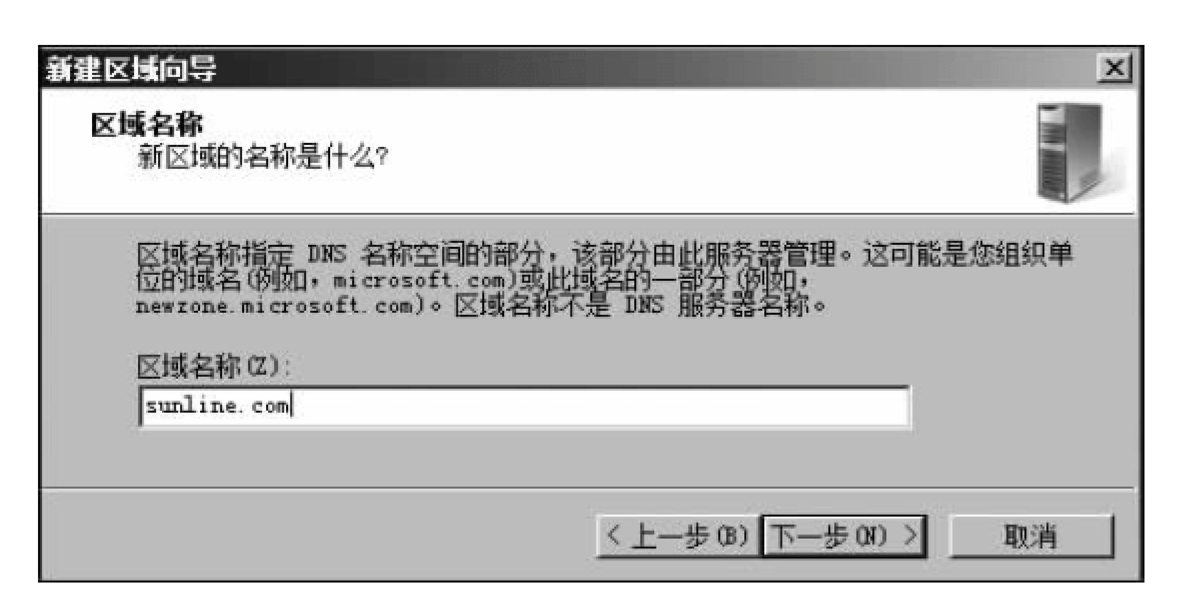


图 8-40　添加区域名称

（10）在“新建区域向导”的“区域文件”对话框中，创建新的区域文件，文件名为 sunline.com.dns，如图 8-41 所示。



图 8-41　创建新的区域文件

（11）在“新建区域向导”的“动态更新”对话框中，选择“不允许动态更新”单选按钮，如图 8-42 所示。

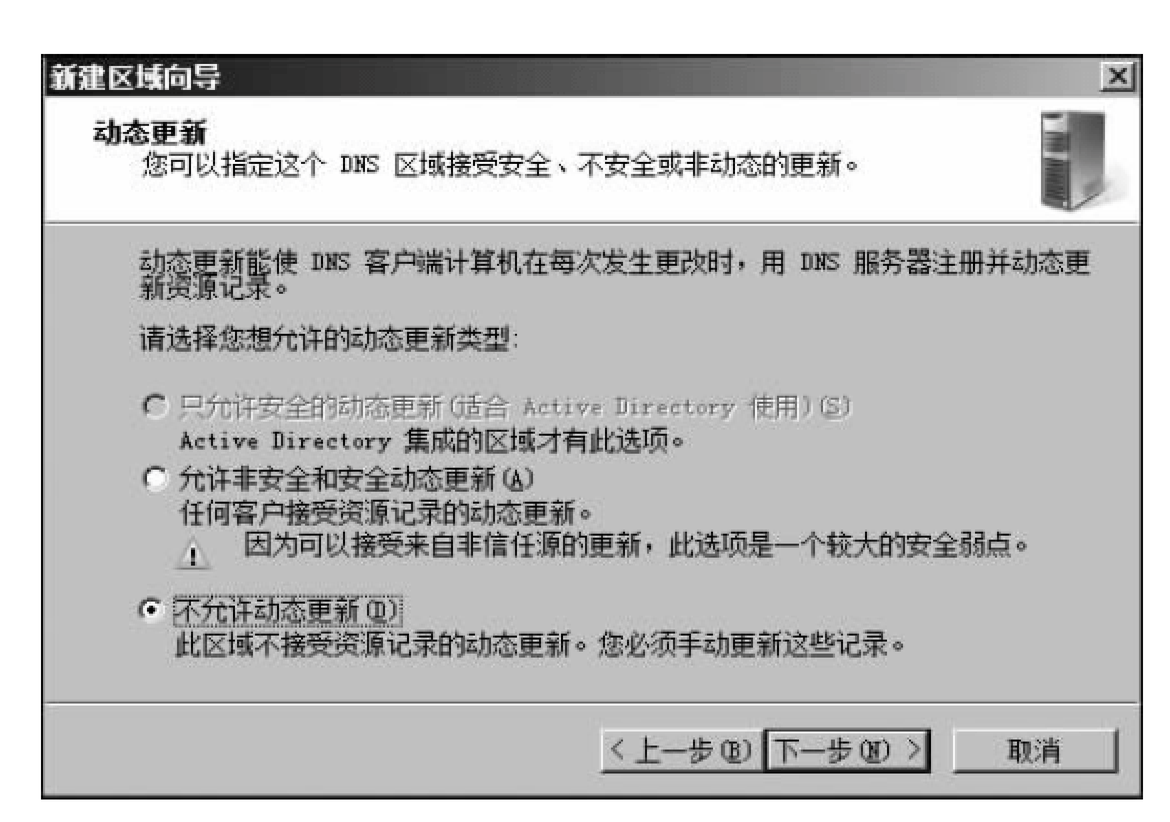


图 8-42　不允许动态更新

（12）完成新建区域向导，如图 8-43 所示。



图 8-43　完成新建区域向导

（13）打开“服务器管理器”窗口，在“DNS 服务器”的“正向查找区域”可以看到正向解析项 sunline.com，如图 8-44 所示。

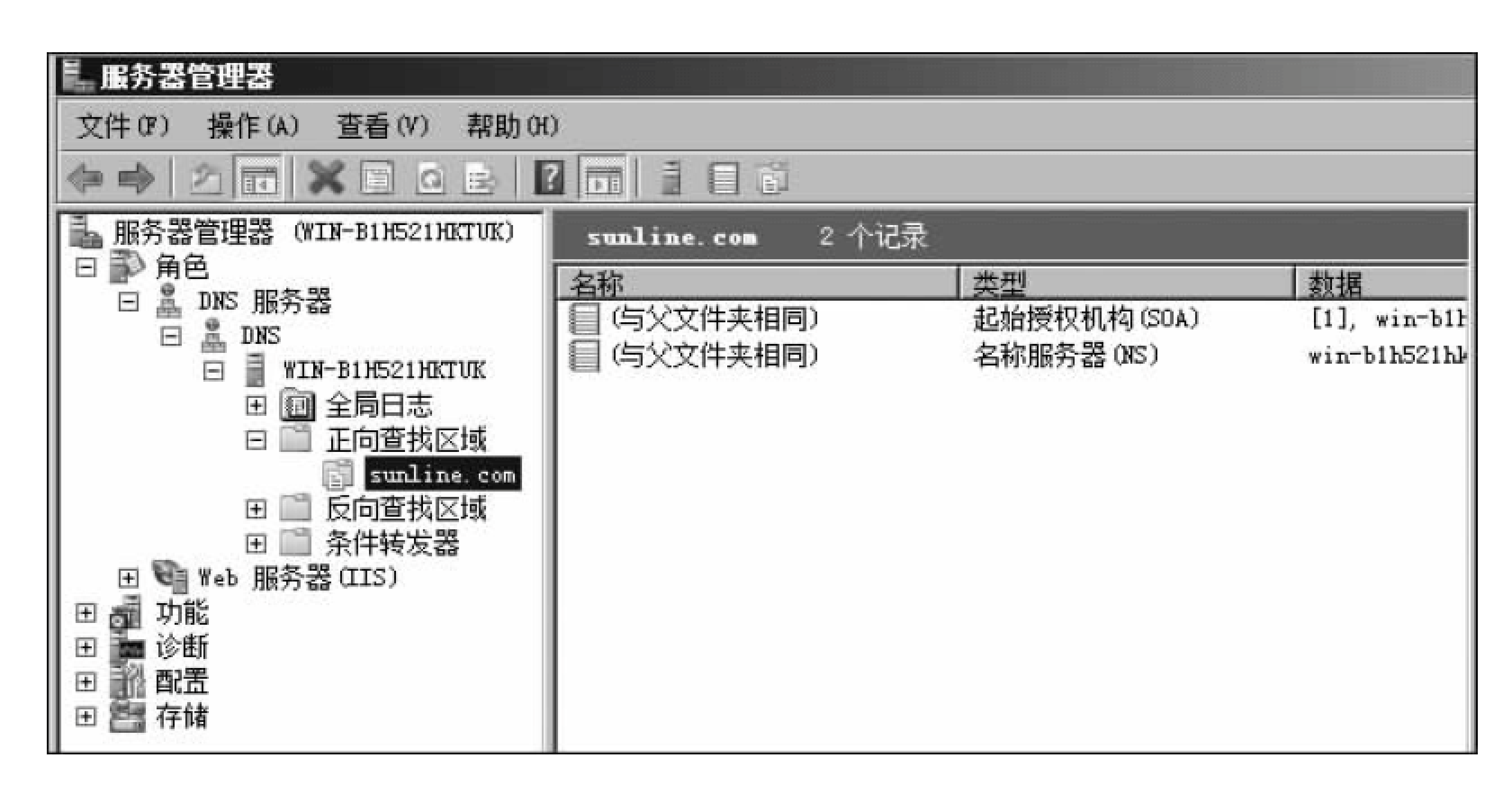


图 8-44　正向查找区域

（14）为解析项配置主机。右击正向解析项 sunline.com，在快捷菜单中选择“新建主机”命令，如图 8-45 所示。

（15）在“新建主机”对话框中，在“名称”文本框中输入主机名称，如 www，在“IP 地址”文本框中输入主机对应的 IP 地址，如图 8-46 所示。

（16）单击“添加主机”按钮，提示主机记录创建成功，如图 8-47 所示。

（17）单击“确定”按钮，完成主机记录 www.sunline.com 的创建。按照同样的步骤，可以添加多个主机记录。设置客户端网络本地连接首选 DNS 为新建主机 DNS 地址，在浏览器地址栏输入 www.sunline.com，验证 DNS 服务器，如图 8-48 所示。

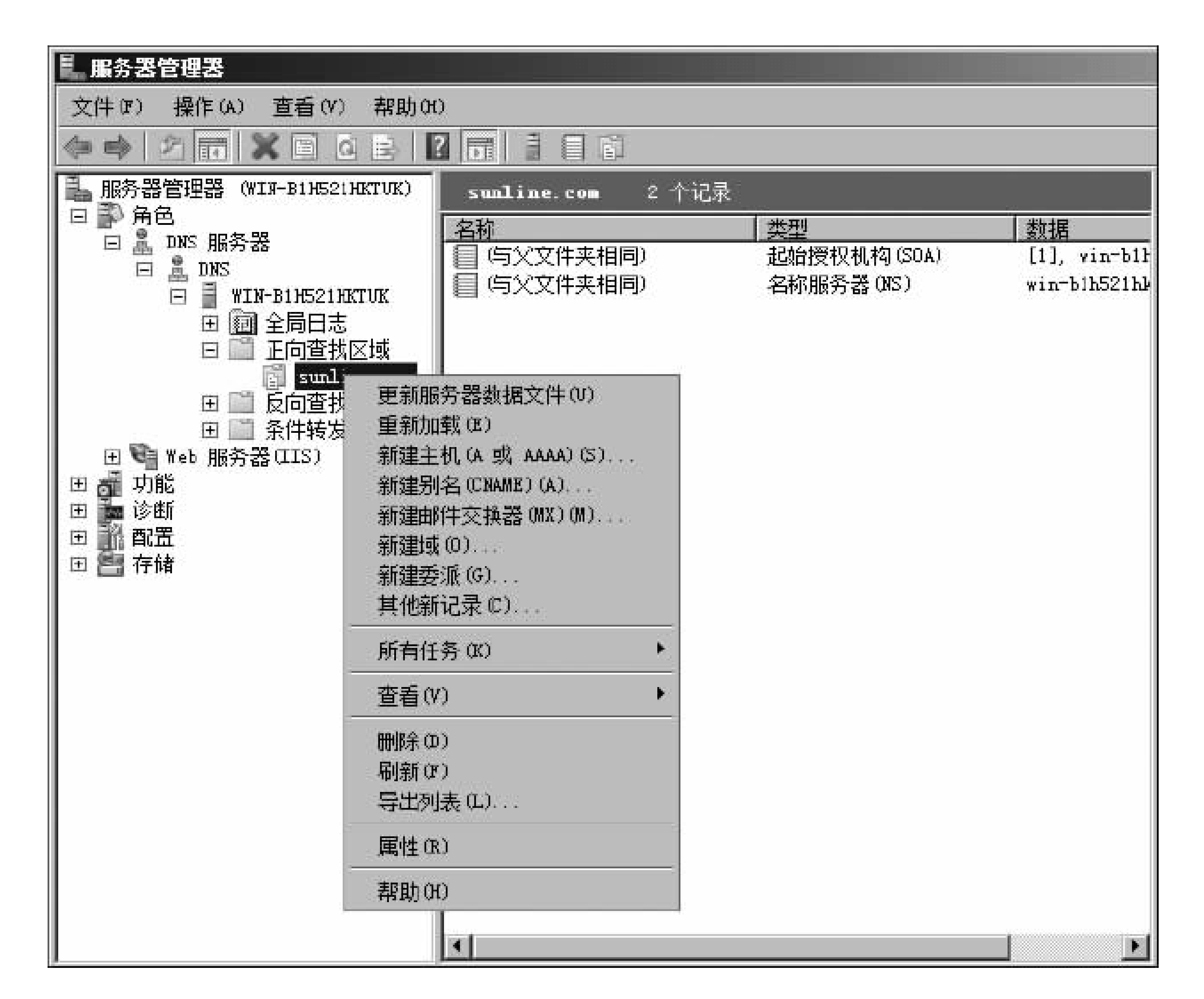


图 8-45　新建主机



图 8-46　新建主机

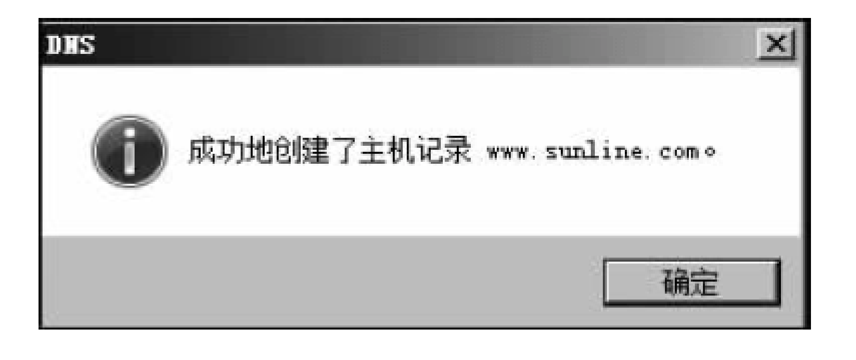


图 8-47　主机记录创建成功



图 8-48　域名验证

（18）DNS解析验证。在客户端计算机上用Nslookup命令解析www.sunline.com，能够正常解析出IP地址，则DNS服务器解析正常，如图8-49所示。



图8-49 Nslookup命令解析IP地址

8.5 DHCP服务器配置与管理

8.5.1 DHCP服务及其工作原理

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)是一个局域网的网络协议，使用UDP协议工作，主要有两个用途：为作用域内的网络自动分配IP地址，对网络内所有计算机进行集中管理。

为了实现IP地址的自动分配，首先需要在指定的一台或多台计算机上安装DHCP服务，提供IP地址的自动分配功能，这些计算机称作DHGP服务器。把希望自动获取IP地址的计算机配置为能够自动请求DHCP服务，这些计算机称作DHCP客户机。这样，当DHCP客户机启动时，会在网络中自动寻找DHCP服务器并且向它们提出租用IP地址的请求，DHCP服务器响应客户机的请求并且为它们自动分配所需要的IP地址，从而实现了IP地址的自动分配。

DHCP服务的工作流程可分为以下4步：客户机请求IP(DHCP discover)，服务器响应(DHCP offer)，客户机获取IP(DHCP request)，服务器确认IP租约(DHCP ack/DHCP nack)。其工作原理如图8-50所示。

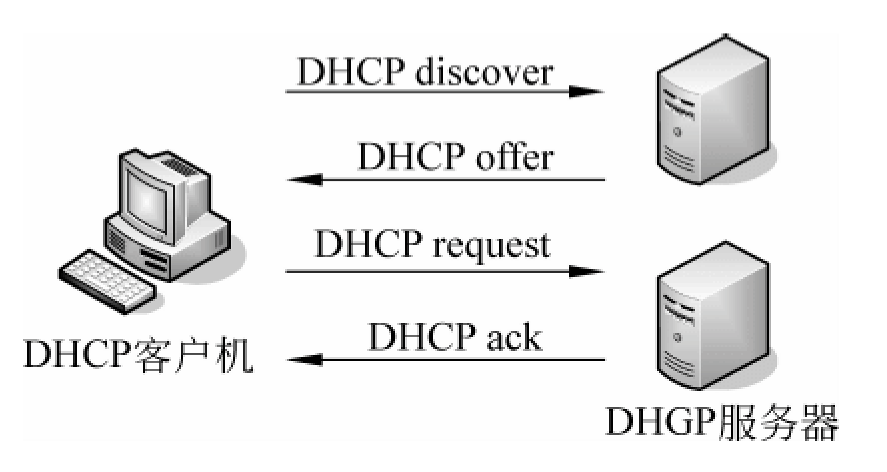


图8-50 DHCP工作原理

8.5.2 DHCP 服务器的安装配置

(1) 选择“开始”→“管理工具”→“服务器管理器”，打开“服务器管理器”窗口，添加服务器角色，勾选“DHCP 服务器”复选框，如图 8-51 所示。



图 8-51 选择 DHCP 服务器

(2) 添加角色向导进入“DHCP 服务器”对话框，显示“DHCP 服务器简介”与“注意事项”等信息，如图 8-52 所示。

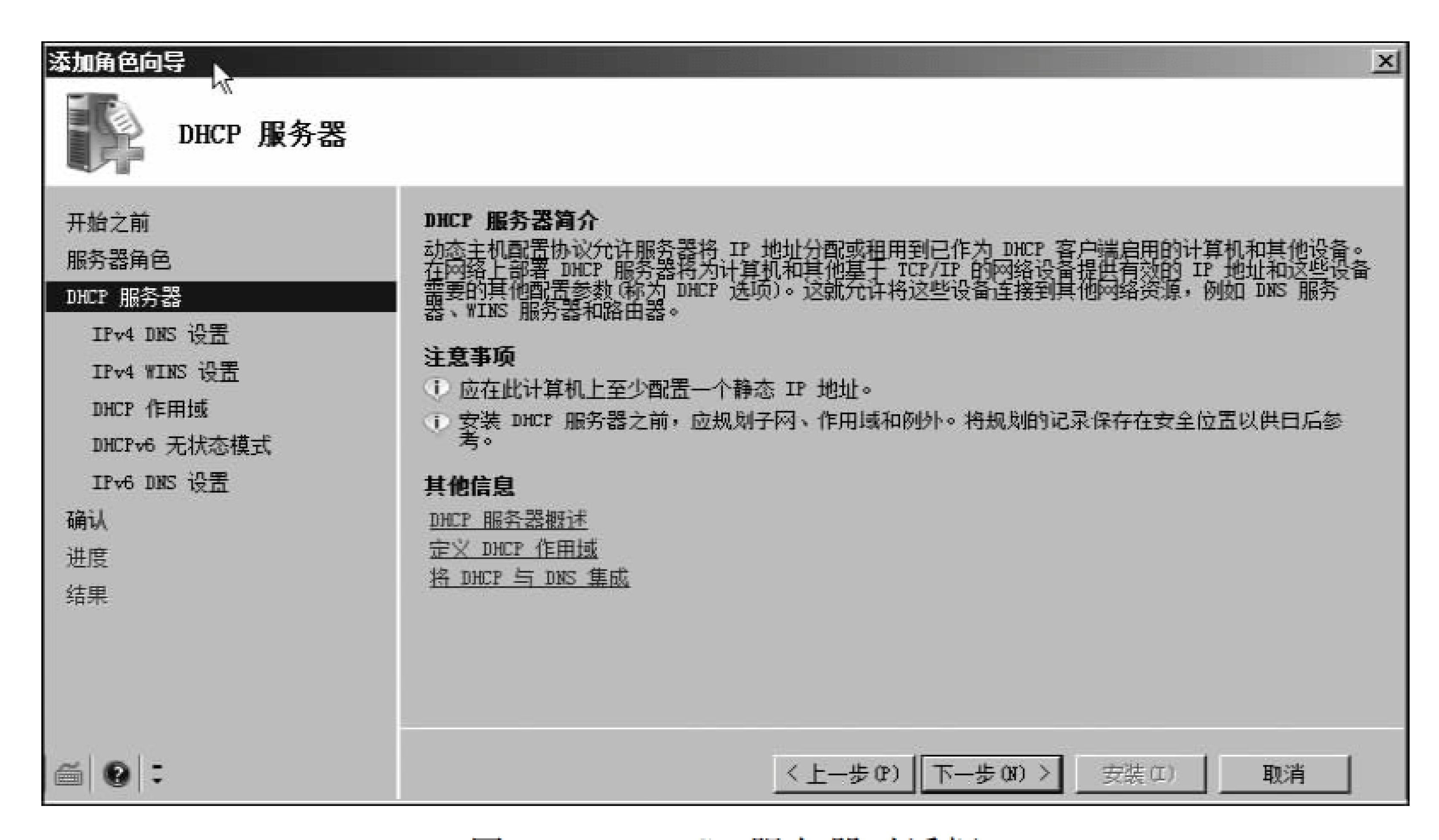


图 8-52 DHCP 服务器对话框

(3) 选择网络连接绑定，即确定 DHCP 服务器 IP 地址，如图 8-53 所示。

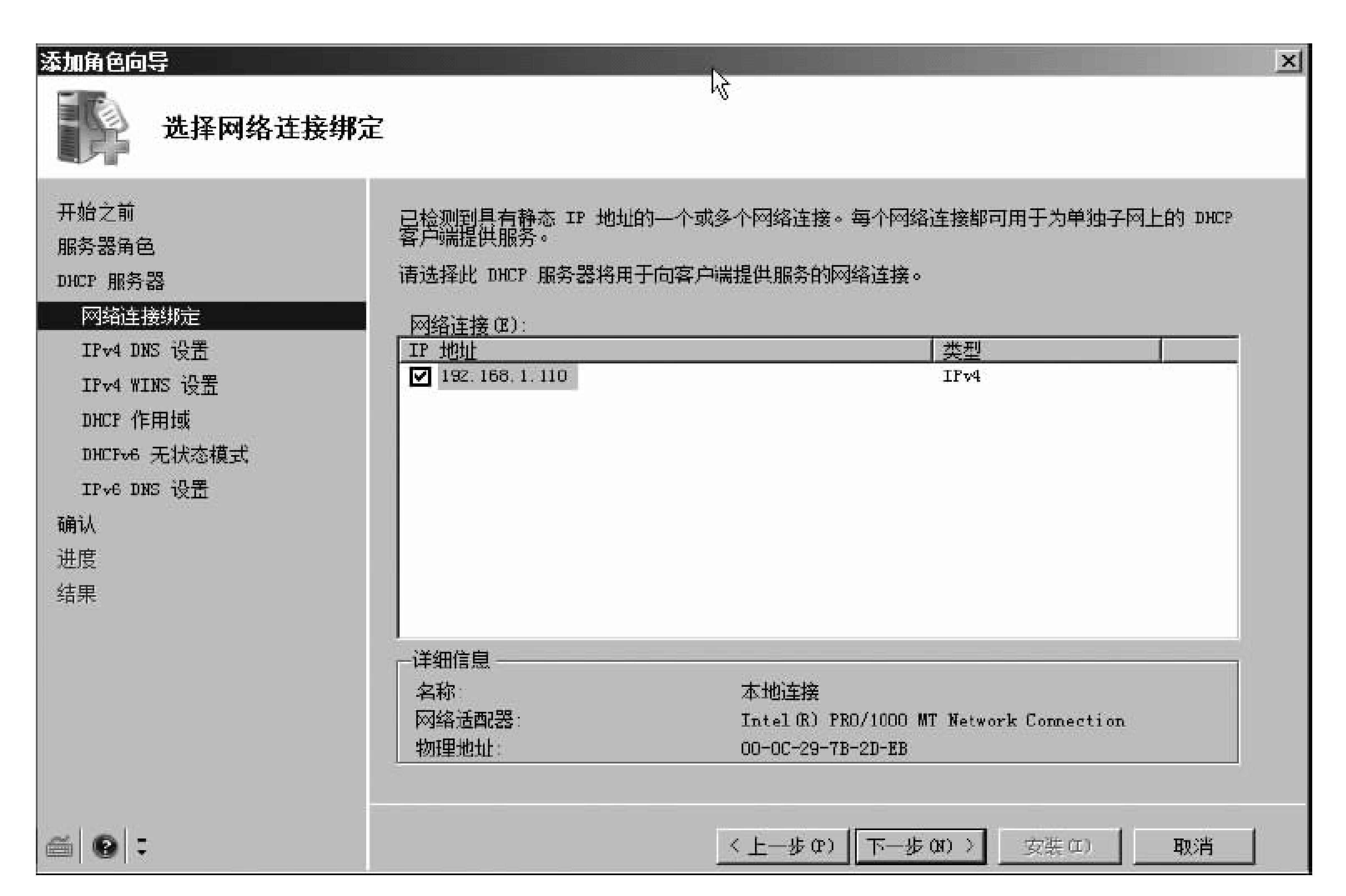


图 8-53　服务器 IP 地址绑定

(4) 输入 DNS 服务器“父域”及“首选 DNS 服务器 IPv4 地址”，实现创建 DHCP 作用域，如图 8-54 所示。

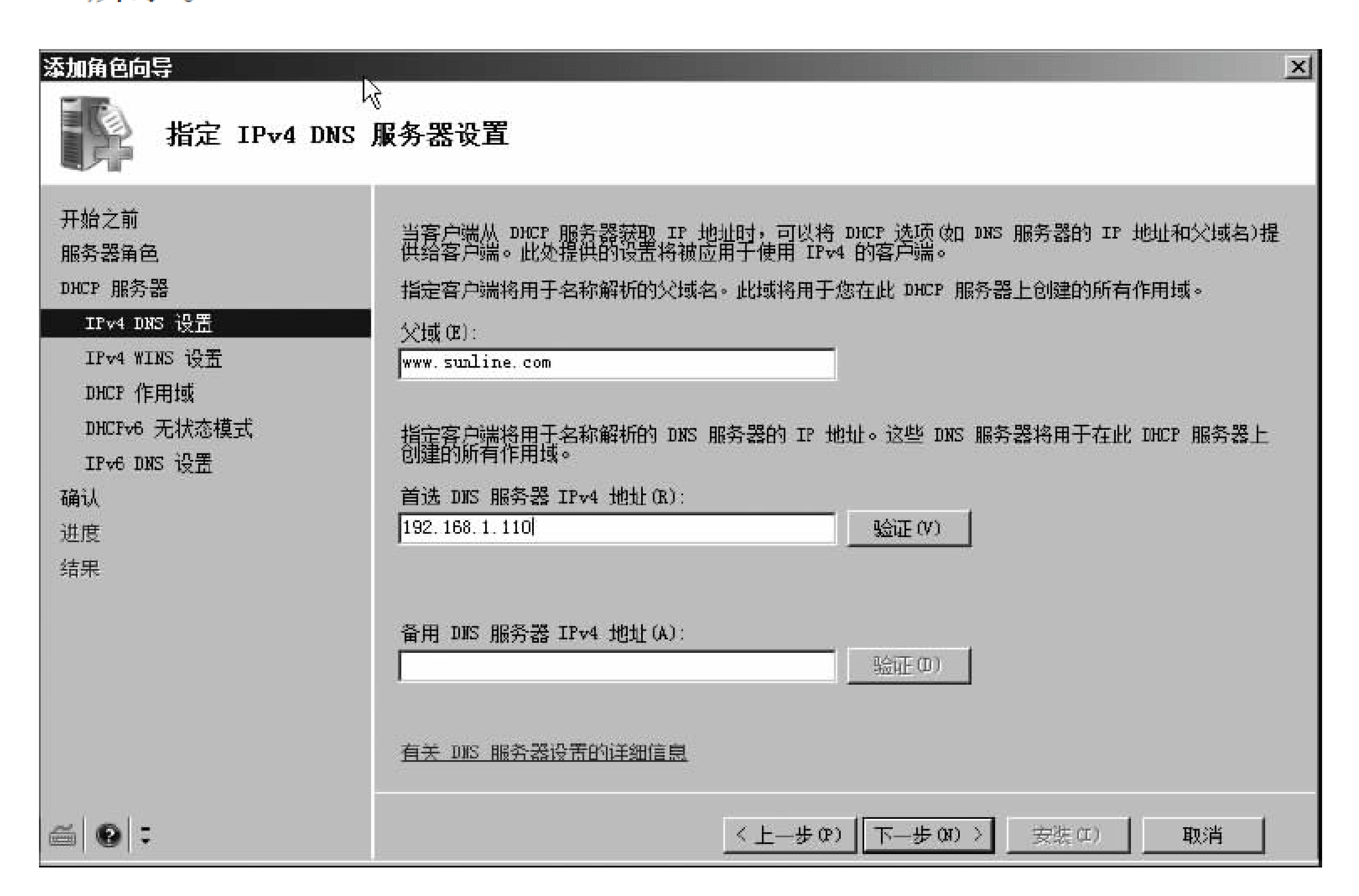


图 8-54　DNS 服务器设置

(5) 添加 DHCP 服务器“作用域名称”与客户端 IP 地址分配范围，如图 8-55 所示。

(6) 确认安装选择，如图 8-56 所示。

(7) DHCP 服务器安装完成，如图 8-57 所示。

(8) 进入服务器管理器，打开 DHCP 服务器，查看作用域是否激活，进入地址租用池可以看到客户端地址租用列表，如图 8-58 所示。

添加作用域

作用域是网络可能的 IP 地址范围。只有创建作用域后，DHCP 服务器才能将 IP 地址分配给各个客户端。

作用域名称(S): SHL
起始 IP 地址(T): 192.168.1.11
结束 IP 地址(E): 192.168.1.200
子网掩码(U): 255.255.255.0
默认网关(可选)(D): 192.168.1.1
子网类型(B): 有线(租用持续时间将为 6 天)

☑ 激活此作用域(A)

确定 取消

图 8-55 添加 DHCP 作用域

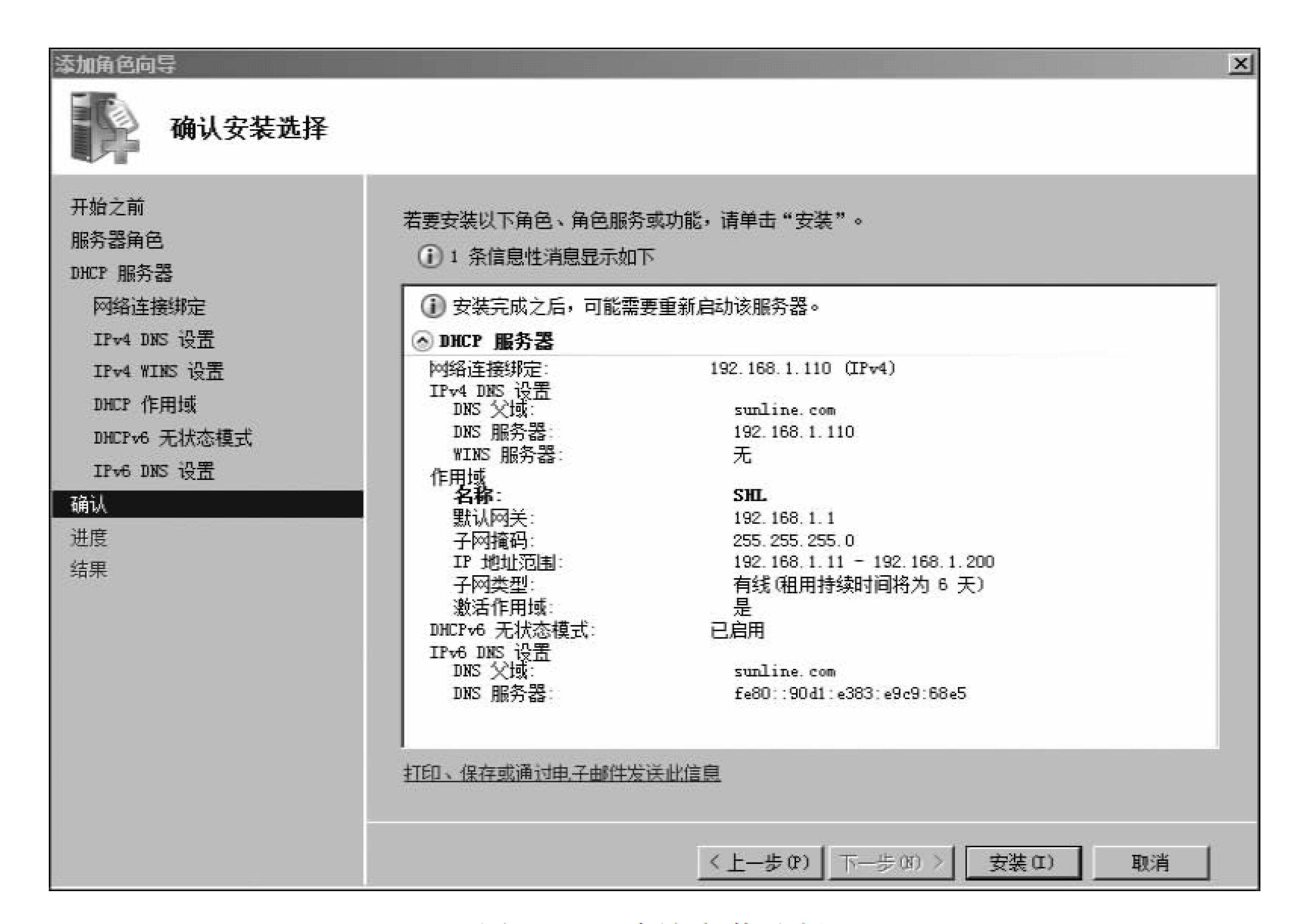


图 8-56 确认安装选择



图 8-57 DHCP 安装完成



图 8-58　激活作用域

(9) 查看地址池中的 IP 地址分发范围，可以对地址池中分发的 IP 地址进行修改，如图 8-59 所示。

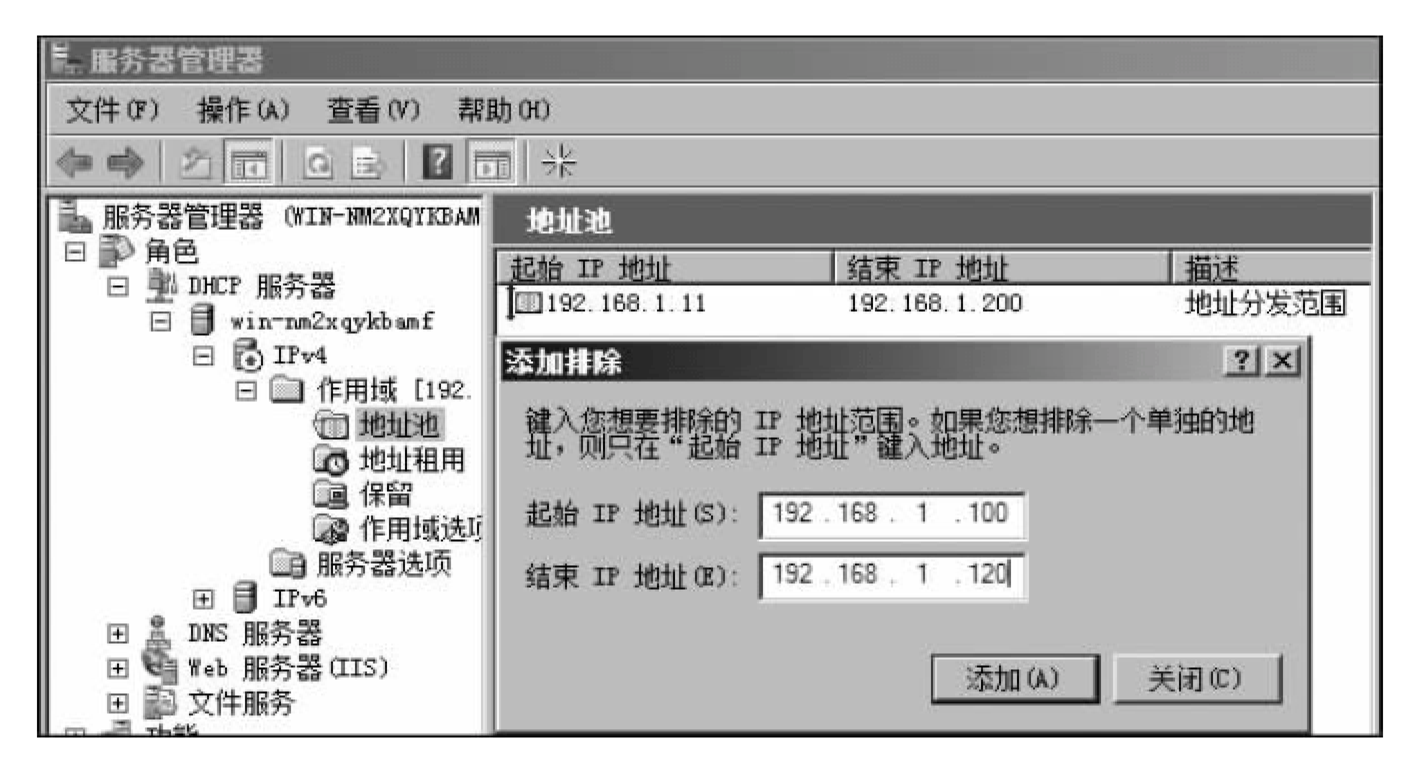


图 8-59　添加排除

(10) 进入 DHCP 服务器客户机，查看"本地连接"中网络连接的详细信息，如图 8-60 所示。



图 8-60　DHCP 提供网络服务

(11) 根据实际网络工作需要，对 DHCP 服务器作用的 IP 地址范围以及排除 IP 地址范围进行调整。

8.6 电子邮件服务

8.6.1 电子邮件服务原理

电子邮件服务可以说是网络应用服务中最便捷、最实用的服务之一。电子邮件的工作模式是客户/服务器模式。每份电子邮件的传输都要涉及收发双方，发送方构成客户端，而接收方构成服务器。服务器开辟有众多用户的电子信箱，发送方通过邮件客户程序将编辑好的电子邮件向邮局服务器发送，一般通过 SMTP 协议实现。邮局服务器识别接收者的地址，并向管理该地址的邮件服务器调用 POP3 协议实现发送消息。邮件服务器将消息存放在接收者的电子信箱内，并告知接收者有新邮件到来。接收者通过邮件客户程序连接到服务器后，就会看到服务器的通知，进而打开自己的电子信箱来查收邮件。

电子邮件在发送与接收过程中都要遵循 SMTP、POP3 等协议，SMTP(Simple Mail Transfer Protocol，简单邮件传输协议)和 POP3(Post Office Protocol，邮局协议)，这些协议确保了电子邮件在各种不同系统之间的传输。SMTP 是 Internet 协议集中的邮件标准。POP3 可允许 E-mail 客户向某一 SMTP 服务器发送电子邮件，另外，也可以接收来自 SMTP 服务器的电子邮件。

通常 Internet 上的个人用户不能直接接收电子邮件，而是通过申请 ISP 主机的一个电子信箱，由 ISP 主机负责电子邮件的接收。一旦有用户的电子邮件到来，ISP 主机就将邮件移到用户的电子信箱内，并通知用户有新邮件。ISP 主机起着邮局的作用，管理着众多用户的电子信箱。每个用户的电子信箱实际上就是用户所申请的账号名称。每个用户的电子邮件信箱都要占用 ISP 主机一定的空间容量，由于这一空间是有限的，因此用户要定期查收和阅读电子信箱中的邮件，以便腾出空间来接收新的邮件。

8.6.2 邮件服务安装与管理

与 Windows Server 操作系统同期推出的邮件服务是 Microsoft Exchange Server，由于 Exchange 配置与管理相对复杂，市场上有许多公司开发了专用邮件服务软件，目前大多数用户选择专用邮件服务器软件构建内部组织的邮件系统。

下面介绍一款邮件服务器软件。

1. Foxmail Server 的安装与设置

Foxmail Server 是一个功能强大、管理灵活的电子邮件服务器软件，完全基于 Web 的管理，可以构建基于 SSL 加密的电子邮件系统，同时支持 C/S 和 C/S/S 两种结构的 E-mail 服务。

(1) 运行 Foxmail Server 软件安装程序，输入产品编号、授权用户数以及产品序列号，如图 8-61 所示。



图 8-61 安装 Foxmail Server 测试版

（2）选择 Foxmail Server 软件安装路径，如图 8-62 所示。

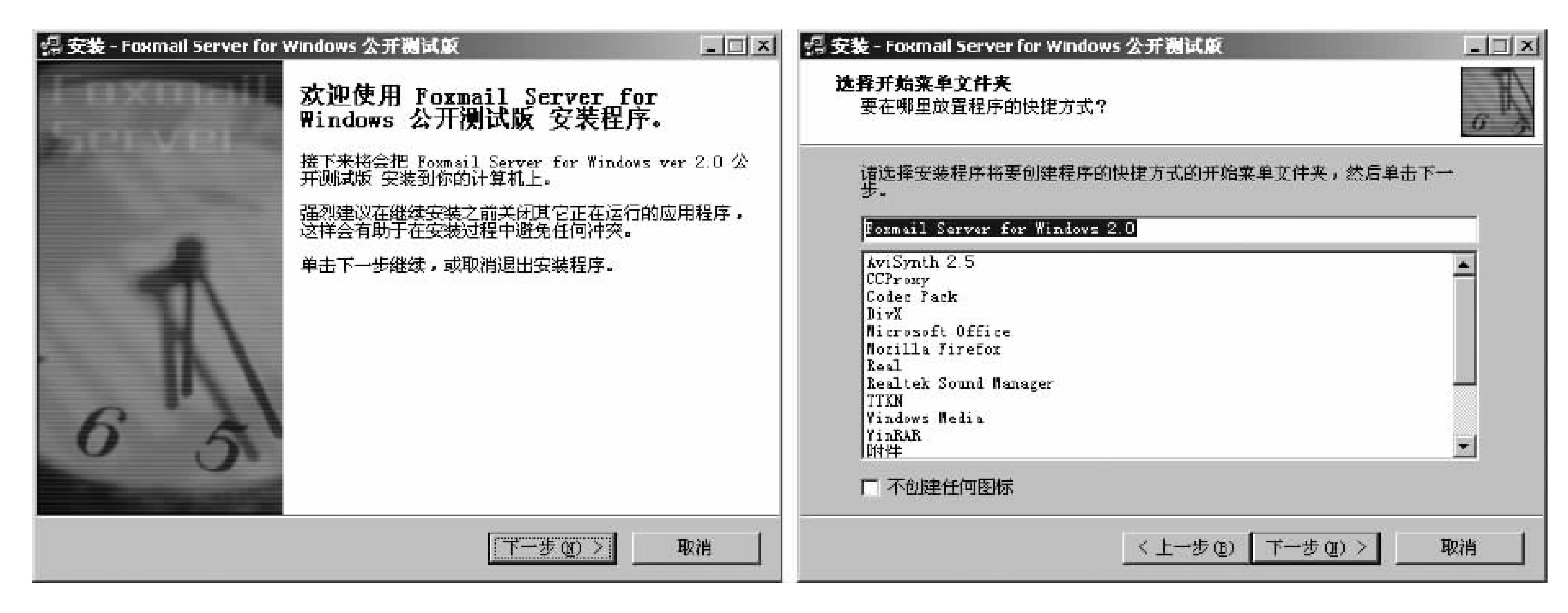


图 8-62 选择安装路径

（3）Foxmail Server 软件开始自动安装，如图 8-63 所示。



图 8-63 软件安装

(4) 进行应用程序设置，邮件服务器域名为 sunline.com，如图 8-64 所示。

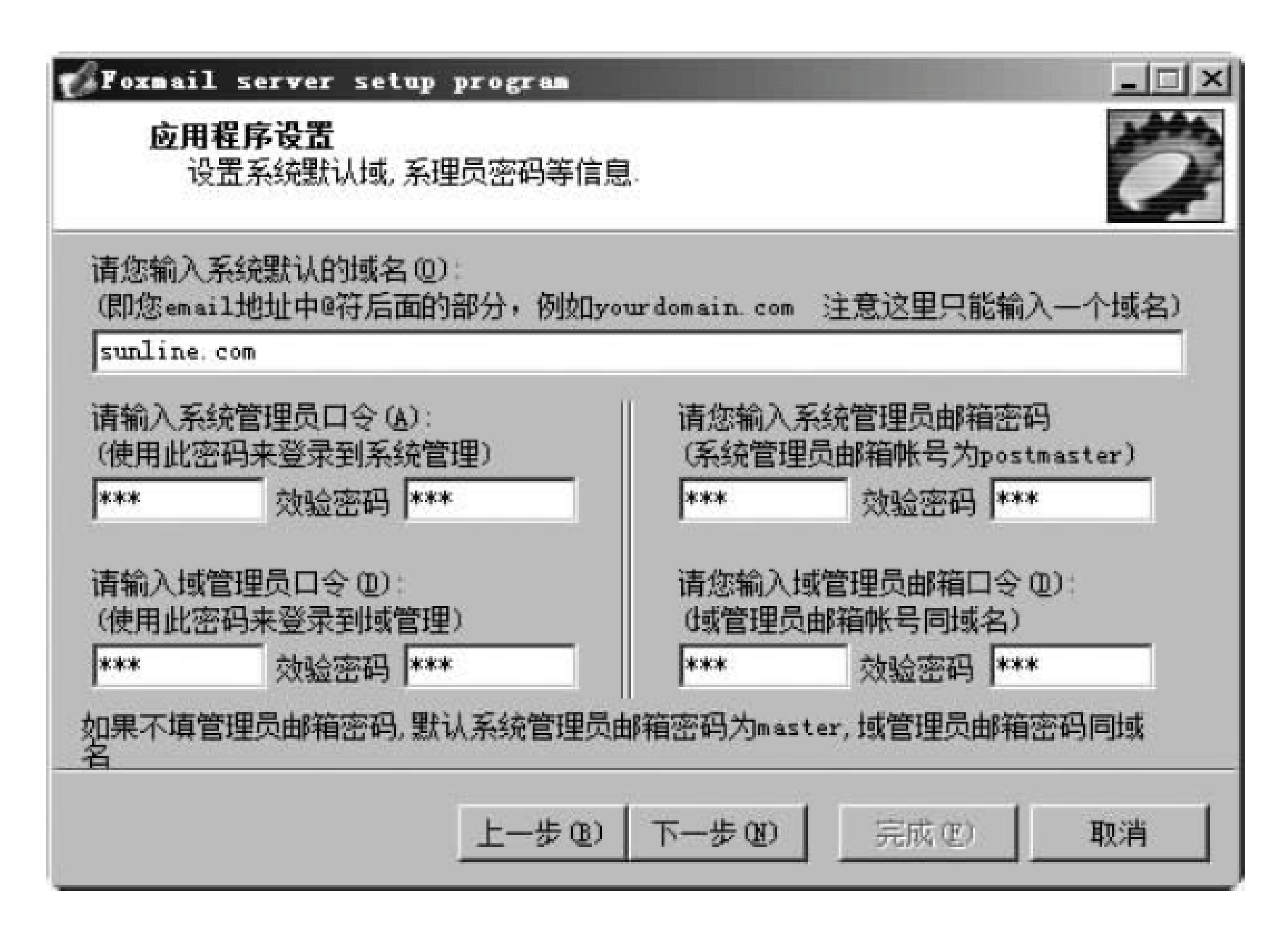


图 8-64 应用程序设置

(5) 进行邮件服务器网络设置，设置 DNS、SMTP 和 POP3 等端口信息，如图 8-65 所示。



图 8-65 邮件服务器网络设置

(6) 进行 IIS 设置，设置 Foxmail Server WebMail 依附的 Web 站点与路径，如图 8-66 所示。

(7) Foxmail Server 安装完成，如图 8-67 所示。

2. 电子邮件服务器新用户注册

Foxmail Server 配置过程中，系统会将用户所选择的"默认 Web 站点"的主目录和文档指向电子邮件服务器，因此当在客户机浏览器的地址栏输入服务器的 IP 地址会自动进入电子邮件服务器的登录界面。





图 8-66　设置 WebMail 依附站点



图 8-67　Foxmail Server 安装完成

(1) Foxmail Server 新用户注册。单击“新用户注册”按钮,在“新用户注册”对话框中输入用户个人基本资料和账号信息,如图 8-68 所示。

(2) Foxmail Server 注册成功,如图 8-69 所示。

至此,使用 Foxmail Server 搭建电子邮件服务器已完成,可以通过远程访问电子邮件服务器注册邮箱,并进行邮件收发。





图 8-68　新用户注册



图 8-69　注册成功

3. 登录电子邮件服务器收发电子邮件

(1) 客户端通过电子邮件服务器登录电子邮箱，如图 8-70 所示。

(2) 发邮件，输入收件人地址等信息，如图 8-71 所示。



图 8-70 登录邮箱



图 8-71 发邮件

（3）收邮件，登录电子邮件箱并打开收件箱，查看邮件信息，如图 8-72 所示。



图 8-72 接收邮件

4. 管理邮件服务器

对 Foxmail Server 邮件服务器的管理分为系统管理和域管理两个层面。在系统管理中进行的设置将对邮件服务器生效，而在域管理中进行的设置仅对选定的域有效。用户可以通过两种方式管理邮件服务器，即“登录 WebMail 管理页面”和“登录本机管理程序”。

8.7 本章小结

网络操作系统的两大功能是网络通信与网络服务。网络操作系统具有许多网络服务功能，IIS 功能是建立强大、灵活而安全的 Internet 和 Intranet 站点的基础。

WWW 是一种建立在 Internet 上的全球性的、交互的、动态多平台、分布式信息系统，它允许用户在一台计算机上通过 Internet 访问另一台计算机上的信息。

FTP 即文本传输协议，是 Internet 提供的基本服务之一。

DNS 域名系统是在域名服务器中保存作用域网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址的服务功能。

DHCP 是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：给内部网络自动分配 IP 地址，对网络内所有计算机进行集中管理。

综合训练

一、理论题

1. 选择题

(1) IIS 的功能是建立强大、灵活而安全的(　　)和 (　　)站点的基础。

A. Internet　　B. HTTP　　C. SMTP　　D. Intranet

(2) 万维网是一种建立在 Internet 上的信息系统，简称(　　)。

A. Web　　B. WWW　　C. World　　D. Wide

(3) FTP 是 Internet 提供的基本服务之一 ，即(　　)协议。

A. 文件传输　　B. 文本传输　　C. 邮件传输　　D. 文件系统

(4) DNS 域名系统是将域名转换为(　　)的服务功能。

A. 二进制　　B. 十进制　　C. 虚拟机　　D. IP 地址

(5) DHCP 是一个局域网的网络协议，使用(　　)协议工作。

A. TCP　　B. HTTP　　C. SMTP　　D. UDP

2. 填空题

(1) IIS 的设计目的是建立一套集成的服务器服务，支持________、________和

________等协议。

（2）WWW是以________方式组织网络多媒体信息。

（3）WWW服务软件以________与________为基础。

（4）Web站点之间可以互相链接________、________、________和________等信息。

（5）DHCP有两个主要用途：给内部网络________，对网络内所有计算机进行________。

3. 简答题

（1）简述Web服务及其工作原理。

（2）简述DHCP服务及其工作原理。

二、实践题

1. 模拟搭建企业内网Web服务系统

菲耶有限公司现有员工120名，公司建有内部网络系统，公司计划建设企业内部网站，员工通过www.feiye.com域名访问公司内部网站，获取公司公开信息，请模拟搭建一个Web服务系统，满足公司需要。

2. 模拟搭建企业内网邮件服务系统

根据菲耶有限公司的实际情况，选择适宜的邮件服务系统，搭建企业内网邮件服务系统。

第 9 章　计算机网络安全与管理

本章主要内容

- 计算机网络安全概述
- 计算机网络安全技术
- 网络安全策略概述
- 网络安全管理与实现

随着 Internet 的迅猛发展和网络社会化的到来，网络已经无所不在地影响着社会的政治、经济、文化、军事、意识形态和社会生活等各个方面。同时，在全球范围内，针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断地增加，网络攻击与入侵行为对国家安全、经济和社会生活产生了极大的威胁。因此，网络安全已成为世界各国共同关注的焦点，对网络安全管理者来说具有挑战性。

9.1　计算机网络安全概述

网络安全是为防范计算机网络中硬件、软件和数据等信息资源遭到主观蓄意破坏、篡改、窃听和假冒等非法访问与获取，减少在客观自然情况下造成的损失，保护网络系统持续有效地工作的策略方案。

计算机网络安全问题涉及许多学科领域，需要在自然科学中找到技术方式，又需要在社会科学领域建立规则。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术和防泄露技术等。因此，计算机网络安全是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。网络安全的组成如图 9-1 所示。

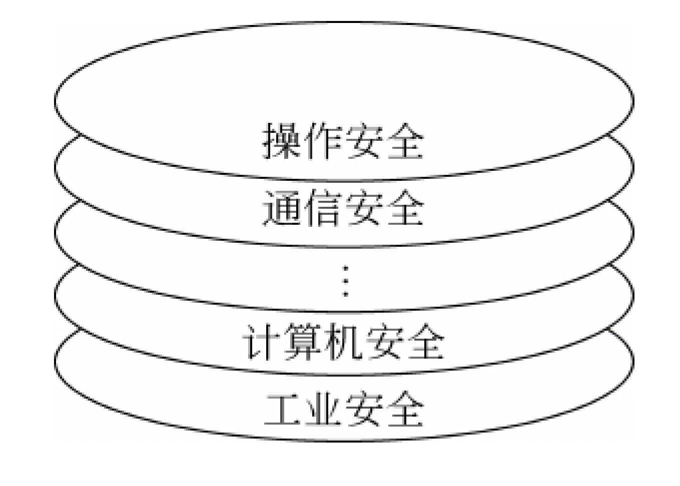


图 9-1　网络安全的组成

目前，网络安全防范的核心是防止主观破坏与窃取。这里需要对“黑客”与“骇客”进行介绍。黑客即英文 Hacker 的音译，早期在计算机界是带有褒义的，原指热心于计算机技术，专门查找计算机系统漏洞或错误的计算机专家，往往是程序设计人员。但到了今天，黑客一词特指利用计算机系统漏洞或错误及其他手段盗取他人计算机系统中的保密信息的人，泛指那些专门利用计算机网络搞破坏或恶作剧者。“骇客”通常是指软件骇客，即英文 Software Cracker，特指专门从事恶意破解商业软件、恶意入侵正常运行系统等破解者。

9.1.1 计算机网络存在的安全隐患

(1) 自然威胁。自然威胁可能来自各种自然灾害、恶劣的场地环境、电磁辐射和干扰、网络设备的自然老化等。这些无目的的事件有时也会直接或间接地威胁网络的安全,影响信息的存储和交换。

(2) 非授权访问。指具有熟练编写和调试计算机程序的技巧,并使用这些技巧来获得非法或未授权的网络或文件访问,侵入他方内部网的行为。网络入侵的目的主要是取得使用系统的存储权限、写权限以及访问其他存储内容的权限,或者是作为进一步进入其他系统的跳板,或者恶意破坏这个系统,使其毁坏而丧失服务能力。例如电子邮件攻击,即攻击者使用邮件炸弹软件和 CGI 程序来向邮箱发送大量垃圾邮件,使网络流量加大,长时间占用处理器,消耗系统资源,从而使系统瘫痪。

(3) 后门和木马。程序在软件的开发阶段,程序员常会在软件内创建后门以便可以修改程序中的缺陷。非法入侵者发展了"后门"这项技术,利用该技术编写有针对性的"后门"程序,借助网络伺机从"后门"进入计算机系统。木马,又称为特洛伊(Trojan horse)木马,其名称取自希腊神话,它是一种基于远程控制的黑客工具,具有隐蔽性和非授权性的特点。

一个木马一般有两个程序,一个是服务器程序,另一个是控制器程序。如果一台计算机被安装了木马服务器程序,那么黑客就可以使用木马控制器程序进入这台计算机,通过命令服务器程序实现控制计算机。

(4) 计算机病毒。在计算机程序中插入的,破坏计算机功能或者破坏数据,影响计算机正常使用,具有能够自我复制功能的一组计算机指令或者程序代码称为计算机病毒。如常见的蠕虫病毒就是以计算机为载体,利用操作系统和应用程序的漏洞主动进行攻击,是一种通过网络传播的恶性病毒。它具有病毒的一些共性,如传播性、隐蔽性、破坏性和潜伏性等,同时具有自己的一些特性,如不利用文件寄生,只存在于内存中,对网络造成拒绝服务。

(5) 网络监听。网络监听是一种工作模式。通过此模式,不管信息的发送方和接收方是谁,主机能够接收本网段在同一通道上传输的信息。当系统进行密码校验时,用户输入的密码从用户端传送到服务器端,攻击者这时就可以在两端进行窃听。如果两台主机通信时没有加密,使用某些网络监听工具就可轻松截取资料,包括账号及口令,从而导致用户隐私遭到很大侵害。

9.1.2 网络安全脆弱性原因

造成计算机网络安全问题的原因很多,但是可以把它们归纳为两大类:即外在的威胁和内在的脆弱性。从威胁的角度来看,潜在的威胁源增多,威胁发生的可能性增大。如果把威胁看作外因,那么系统不安全的内因,也可以说最根本的原因,是计算机网络本身存在脆弱性,而且这种脆弱性问题也越来越严重。

脆弱性是指一个系统可被非预期利用的方面，例如系统中存在的各种漏洞，可能的威胁就可以利用漏洞给系统造成损失。系统遭受损失，最根本的原因在于本身存在脆弱性。因为攻击者只有利用了系统的脆弱性，攻击才能成功。系统的脆弱性包括系统最初存在的脆弱性和后来增加的安全措施存在的脆弱性。

完整地描述脆弱性是比较困难的，这是源自于：编程过程中出现逻辑错误是很普通的现象，这些错误绝大多数是由于疏忽造成的；数据处理比数值计算更容易出现逻辑错误，过小或过大的程序模块比中等程序模块更容易出现错误；脆弱性和具体的系统环境密切相关；在不同种类的软硬件设备中，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各种不同的安全问题；脆弱性问题与时间紧密相关，随着时间的推移，旧的脆弱性会不断得到修补或纠正，新的脆弱性会不断出现，因而脆弱性问题会长期存在。在对脆弱性进行研究时，除了需要掌握脆弱性本身的特征属性，还要了解与脆弱性密切相关的其他对象的特点。脆弱性的基本属性有脆弱性类型、造成的后果、严重程度、环境特征等。与脆弱性相关的对象包括存在脆弱性的软硬件、操作系统、相应的补丁程序和修补脆弱性的方法等。

脆弱性的深层原因是：由于对程序内部操作的不了解，或者没有足够的重视，程序员总是假定他们的程序在任何环境中都正常地运行。当程序员的假设得不到满足，程序内部的相互作用和安全策略产生冲突时，便形成了安全脆弱性。

脆弱性包括环境、受影响的对象、对象所受的影响、影响对象的方式以及外部输入5个部分，通过分析每个作用是否和安全策略相违背，就可以找到产生脆弱性的深层原因。

(1) 环境。一般认为"一个系统"是由"应用程序"和"运行环境"组成的，这样，所有被认为不属于运行程序的代码和部件就属于环境。内部对象以及外部输入之间的相互作用使环境具有动态特征和共享特性。这使程序的安全策略实行起来更加困难并容易发生错误。从安全策略的角度出发，执行每个操作都需要考虑环境实体：环境名称、程序运行的目录、创建的临时项目、内存空间、输入的数据、存储的文件、对象属性、对象性质和网络标志等。

(2) 对象。程序代码和数据空间中的任何一个元素都被认为是一个内部对象。对于一个特定的操作而言，这些对象又构成了内部环境，每个对象就是一个环境实体。这些内部对象有系统设备、用户文件、系统程序、用户程序、网络连接、用户名、域名、网络端口、网络数据包和地址映射等。

(3) 对象所受的影响。程序内部的相互作用导致内部对象的改变，变化包括完全取代、可写、可读、可追加、被创建、被显示、所有权改变、用户权限改变、动态加载和连接、被锁、被调试、被关闭和被终止等。

(4) 影响对象的方式。包括连接或绑定连接、配置错误、修改环境变量、修改编码、改变对象名字、继承不必要的特权、提供不适当的权限、不能正确完成保护机制、使用代理绕过、使用死循环消耗资源和临界选择错误等。

(5) 外部输入。用户通过外部输入直接或间接地影响程序的内部操作，控制程序的运行步骤，从而完成需要的程序功能。一般的输入类型有环境变量、命令行选项、网络数据、临时文件、配置文件、数据文件、系统用户信息和可移动介质等。

9.1.3 网络安全入侵步骤与途径

1. 安全入侵的步骤

安全入侵可以大致分为以下几个步骤：

(1) 获取目标系统的信息。操作系统的类型和版本，主要提供的服务及服务进程的类型和版本，网络拓扑等信息都会给予入侵者帮助。

(2) 获得对系统访问的权限。包括读写文件、运行程序的权限等。只要获得这类权限，系统的安全就已经丧失了。

(3) 获得系统超级用户的权限。利用(2)的权限和系统的漏洞，入侵者可以任意修改文件，运行任何程序，抹去入侵的痕迹，并留下下次入侵的后门，或者干脆毁坏整个系统。

通常，(2)、(3)步之间没有准确的分界，有时入侵者可以直接获得超级用户权限。

2. 安全入侵的途径

从利用的漏洞上划分安全入侵，可以大致分为下面3种：

(1) 网络的漏洞。这些漏洞包括网络传输时对协议的信任以及网络传输的漏洞，比如IP欺骗(篡改信息，使目标机认为信息来自另一台主机)和信息腐蚀(篡改网络上传播的信息)就是利用网络对IP和DNS的信任，而侦听器则利用了网络信息明文传送的弱点。

(2) 服务器的漏洞。利用服务进程的缺陷和配置错误，可以攻击任何向外提供服务的主机。

(3) 操作系统的漏洞。计算机操作系统本身所存在的问题或技术缺陷是主要的入侵途径。

9.2 计算机网络安全技术

9.2.1 网络安全的基本要素

网络安全就是通过计算机技术、通信技术、密码技术和安全技术保护在公用网络中存储、交换和传输信息的可靠性、可用性、保密性、完整性和不可抵赖性的技术。

(1) 安全性。包括以下几个方面：

① 确保系统的可靠性，以避免软件的缺陷成为系统的入侵点。

② 对用户实施访问控制，拒绝其访问超出访问权限的资源。

③ 加密传输和存储的数据，防止重要信息被非法用户理解或修改。

④ 对用户的行为进行实时监控和审计，检查其是否对系统有攻击行为，并对入侵的用户进行跟踪。

⑤ 加强系统的物理安全,防止其他用户直接访问系统。

⑥ 保证人事安全,加强安全教育,防止用户(特别是内部用户)泄密。

(2) 完整性。包括软件完整性和数据完整性。解决如何保护计算机系统内软件和数据不被非法删改的问题。

(3) 保密性。加密是保护数据的一种重要方法,也是保护存储在系统中的数据的一种有效手段,人们通常采用加密来保证数据的保密性。解决如何防止用户非法获取关键的敏感信息,避免机密信息的泄露。

(4) 可用性。指无论何时,只要用户需要,系统和网络资源必须是可用的,尤其是当计算机及网络系统遭到非法攻击时,它必须仍然能够为用户提供正常的系统功能或服务。为了保证系统和网络的可用性,必须解决网络和系统中存在的各种破坏可用性的问题。

(5) 不可抵赖性。也称作不可否认性,在网络信息系统的信息交互过程中,确信参与者的真实同一性。即,所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息,利用递交接收证据可以防止收信方事后否认已经接收的信息。

9.2.2 网络安全的基本内容

从技术角度分析,网络安全的内容大体包括4个方面:

(1) 网络实体安全。如机房的物理条件、物理环境及设施的安全标准,计算机硬件、附属设备及网络传输线路的安装及配置等。

(2) 软件安全。如保护网络系统不被非法侵入,系统软件与应用软件不被非法复制、篡改,不受病毒的侵害等。

(3) 网络数据安全。如保护网络数据不被非法存取,保护其完整一致等。

(4) 网络安全管理。运行时突发事件的安全处理,包括采取计算机安全技术,建立安全管理制度,开展安全审计,进行风险分析等内容。

由此可见,计算机网络安全不仅要保护计算机网络设备安全,还要保护数据安全等,网络安全模型如图9-2所示,其特征是针对计算机网络本身可能存在的安全问题,实施网络安全保护方案,以保证计算机网络自身的安全性为目标。

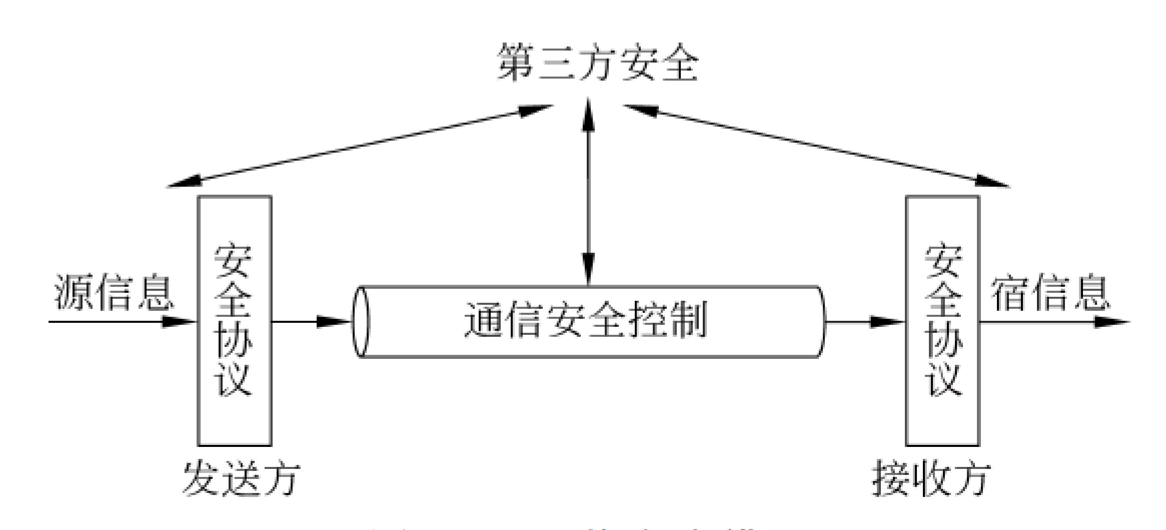


图 9-2 网络安全模型

9.2.3 常用的网络安全技术

1. 防火墙(firewall)技术

防火墙技术是指网络之间通过预定义的安全策略,对内外网通信强制实施访问控制的安全应用措施。它对两个或多个网络之间传输的数据包按照一定的安全策略来实施检查,以决定网络之间的通信是否被允许,并监视网络运行状态。由于它简单实用且透明度高,可以在不修改原有网络应用系统的情况下达到一定的安全要求,所以被广泛使用。

目前,市场上防火墙产品很多,一些厂商还把防火墙技术并入其硬件产品中,即在其硬件产品中采取功能更加先进的安全防范机制。可以预见,防火墙技术作为一种简单实用的网络信息安全技术将得到进一步发展。然而,防火墙也并非人们想象的那样不可渗透。据统计,曾遭受过黑客入侵的网络用户有三分之一是有防火墙保护的,也就是说,要保证网络信息的安全,还必须有其他一系列措施,例如对数据进行加密处理。

需要说明的是,防火墙只能抵御来自外部网络的侵扰,而对企业内部网络的安全却无能为力。要保证企业内部网的安全,还需通过对内部网络的有效控制和管理来实现。

2. 数据加密技术

数据加密技术就是对信息进行重新编码,从而隐藏信息内容,使非法用户无法获取信息的真实内容的一种技术手段。数据加密技术是为提高信息系统及数据的安全性和保密性,防止秘密数据被外部破析所采用的主要手段之一。

数据加密技术按作用不同可分为数据存储、数据传输、数据完整性的鉴别以及密钥管理技术4种。数据存储加密技术以防止在存储环节上的数据失密为目的,可分为密文存储和存取控制两种;数据传输加密技术的目的是对传输中的数据流加密,常用的有线路加密和端口加密两种方法;数据完整性鉴别技术的目的是对介入信息的传送、存取、处理人的身份和相关数据内容进行验证,达到保密的要求,系统通过对比验证对象输入的特征值是否符合预先设定的参数,实现对数据的安全保护。

数据加密技术主要是通过对网络数据的加密来保障网络的安全可靠性,能够有效地防止机密信息的泄漏。另外,它也广泛地应用于信息鉴别、数字签名等技术中,用来防止电子欺骗,这对信息处理系统的安全起到了极其重要的作用。

3. 系统容灾技术

一个完整的网络安全体系,只有防范和检测措施是不够的,还必须具有灾难容忍和系统恢复能力。因为任何一种网络安全设施都不可能做到万无一失,一旦发生漏防漏检事件,其后果将是灾难性的。此外,天灾人祸、不可抗力等所导致的事故也会对信息系统造成毁灭性的破坏。这就要求即使发生系统灾难,也能快速地恢复系统和数据,才能完整地保护网络信息系统的安全。现阶段主要有基于数据备份和基于系统容错的系统容灾技术。数据备份是数据保护的最后屏障,不允许有任何闪失。但离线介质不能保证安全。

数据容灾通过IP容灾技术来保证数据的安全。数据容灾使用两个存储器，在两者之间建立复制关系，一个放在本地，另一个放在异地。本地存储器供本地备份系统使用，异地容灾备份存储器实时复制本地备份存储器的关键数据。二者通过IP相连，构成完整的数据容灾系统，也能提供数据库容灾功能。

集群技术是一种系统级的系统容错技术，通过对系统的整体冗余和容错来解决系统任何部件失效而引起的系统灾难问题。集群系统可以采用双机热备份、本地集群网络和异地集群网络等多种形式实现，分别提供不同的系统可用性和容灾性。

4. 漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全的技术，它查询TCP/IP各种服务的端口，并记录目标主机的响应，收集关于某些特定项目的有用信息。这项技术的具体实现就是安全扫描程序。

扫描程序可以在很短的时间内查出现存的安全脆弱点。扫描程序开发者利用可得到的攻击方法，并把它们集成到整个扫描中，扫描后以统计的格式输出，便于参考和分析。

5. 物理安全

为保证信息网络系统的物理安全，还要防止系统信息在空间的扩散。通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。为保证网络的正常运行，在物理安全方面应采取如下措施。

（1）产品保障方面：主要指产品采购、运输和安装等方面的安全措施。

（2）运行安全方面：网络中的设备，特别是安全类产品，在使用过程中必须能够从生产厂家或供货单位得到迅速的技术支持服务。对一些关键设备和系统，应设置备份系统。

（3）防电磁辐射方面：所有重要的涉密设备都需安装防电磁辐射产品，如辐射干扰机。

（4）保安方面：主要是防盗、防火等，还包括网络系统的所有网络设备、计算机和安全设备的安全防护。

计算机网络安全是一个综合性和复杂性的问题。面对网络安全行业的飞速发展以及整个社会越来越快的信息化进程，各种新技术将会不断出现和应用。

9.3 网络安全的策略概述

9.3.1 网络安全策略的分类

1. 物理安全策略

物理安全策略的目的是：保护计算机系统、网络服务器和打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非

法进入计算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏是物理安全策略的一个主要问题。目前主要的防护措施有两类：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，这类防护措施又可分为以下两种：一是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；二是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2. 访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。

9.3.2 信息加密与传输安全策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端到端加密和节点加密 3 种。链路加密的目的是保护网络节点之间的链路信息安全；端到端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程由许多复杂的加密算法来具体实施，它以很小的代价提供很大的安全保护。在多数情况下，信息加密是保证信息机密性的唯一方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

数据传输所涉及的因素包括两点：数据的发送端/接收端和数据传输的通道。针对数据传输的因素，传输数据信息丢失的原因大致可以划分为两类：一类是非法用户对数据的发送端和接收端进行更改以窃取数据，另一类是非法用户在数据通道上截取传输数据。

针对以上两种数据安全问题，数据传输安全策略应用从以下两个方面进行。第一，利用加密技术对数据进行加密，即系统提供一个安全的加密通道；第二，利用公共密钥签名和数据证书对用户端和服务器进行身份验证。

9.3.3 安全策略的配置

开放式网络环境下用户的合法权益通常受到两种方式的侵害：主动攻击和被动攻击，主动攻击包括对用户信息的窃取以及对信息流量的分析。网络安全策略模型如图 9-3

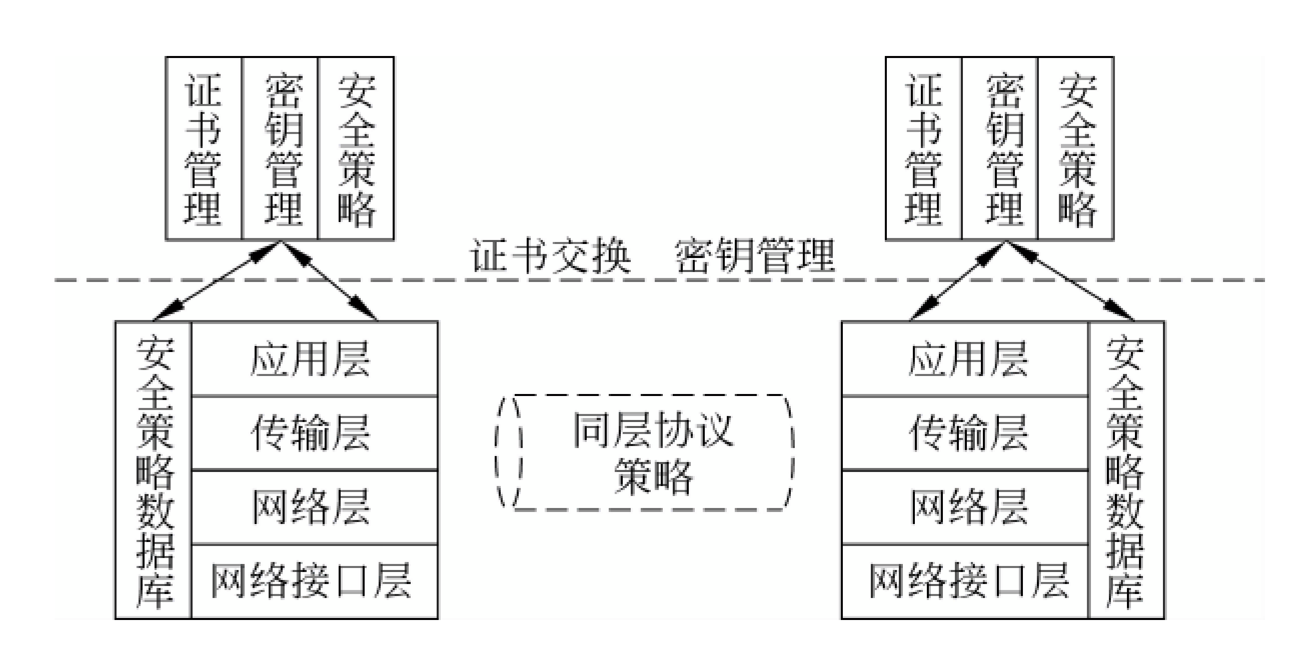


图 9-3 网络安全策略模型

所示。根据用户对安全的需求，可以采用以下保护：

（1）身份认证。检验用户的身份是否合法，防止身份冒充及对用户实施访问控制；数据完整性鉴别，防止数据被伪造、修改和删除。

（2）信息保密。防止用户数据被泄露或被窃取，保护用户的隐私。

（3）数字签名。防止用户否认对数据所做的处理。

（4）访问控制。对用户的访问权限进行控制。

（5）不可否认性。也称不可抵赖性，即防止对数据操作的否认。

9.4 网络安全管理与实现

9.4.1 网络安全管理

1. 规范网络应用的社会环境

随着网络技术的深入发展和广泛应用，网络中已出现许多不容回避的道德与法律的问题。需要大力进行网络法律建设，维护网络正常运行，构建道德准则，共建健康的网络环境。

2. 加强技术防范措施

目前，网络互连的协议一般采用 TCP/IP 协议。TCP/IP 协议在制订之初没有把安全考虑在内，所以没有安全可言。协议中存在很多的安全问题，由此人们开始研究各种各样的网络安全技术来保证网络安全。方法主要有两种，一种是制订一个新的安全的网络互连协议，另一种是在兼容目前网络系统的基础上开发网络安全产品来保证网络上的信息安全。目前的解决方法就是采用网络安全技术，比如 VPN、防火墙技术等。

现在解决网络安全问题的一个有效的方法就是在内部网和外部网之间设置防火墙，如图 9-4 所示。防火墙是在内部网与外部网之间建立的一个保护层，网络内部之间的访问根据原有的协议进行，网络内部对外部网络的访问在事先约定的协议授权约束下进行，而外部网络对本地内部网络的访问则受到防火墙的隔离，从而保护了本地的内部网络资源免受外部的非法入侵。

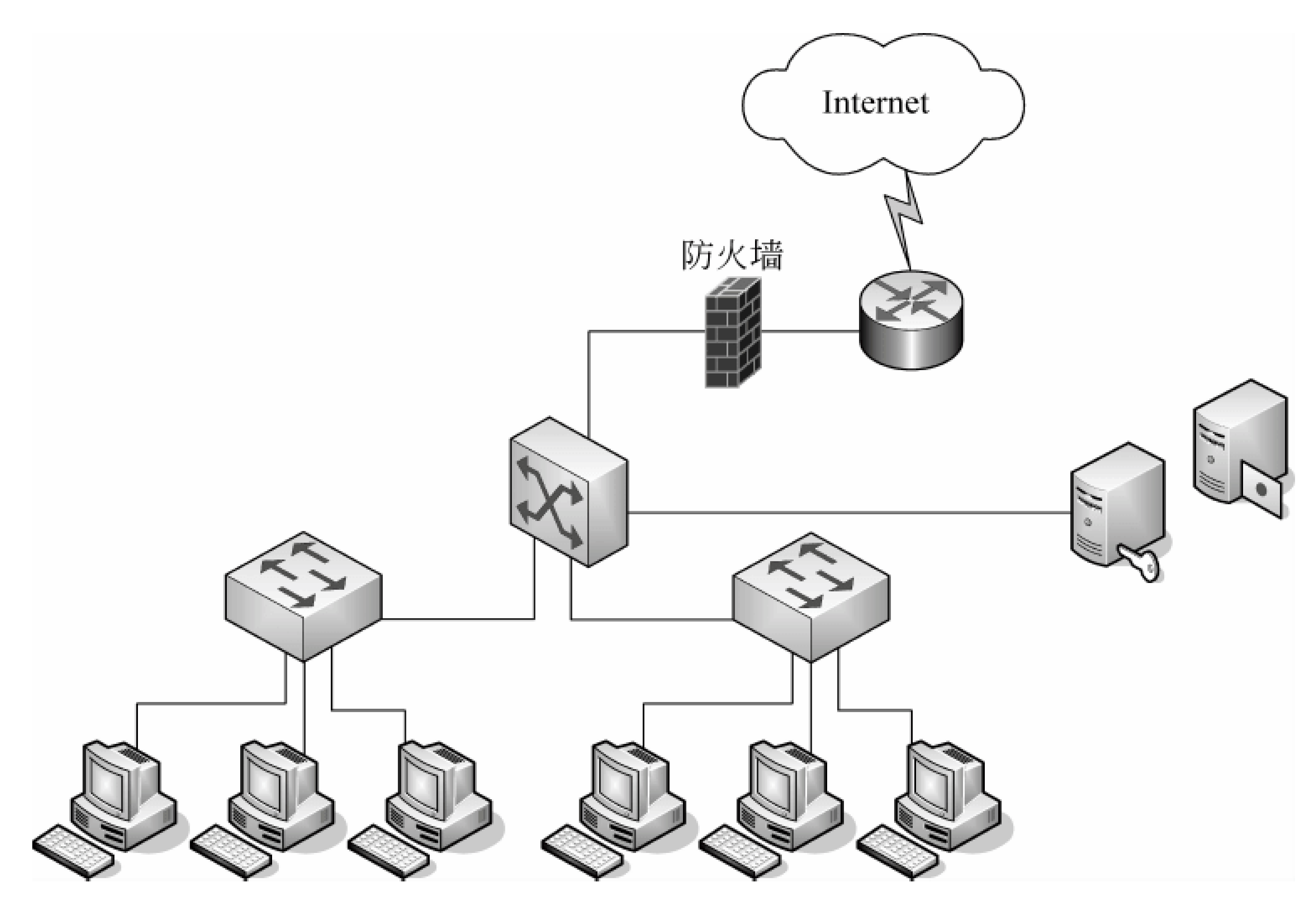


图 9-4　防火墙策略

3. 强化网络监控

随着网络行为的复杂化和网络犯罪的隐蔽性，通过监控技术对于网上敏感信息进行追踪，并对可疑用户行为进行监控，把使用网络的行为管理起来。

4. 增强安全意识

增强用户的网络安全意识，提高网络安全技术，坚持健康、守法地使用计算机网络，自觉抵制不良网络的诱惑。

9.4.2　网络安全实现

1. 采用多层次的防治措施

(1) 单点管理。提出一个集成化的解决方案时，必须要有一个安全管理的聚焦点。

(2) 逻辑上的集成性。所采用的保护措施应在逻辑上是统一的，并能相互配合。

(3) 分布的多层性。最终采用的解决方案应该是多层次的，把相应的防毒部件放在适当的位置，最大限度地发挥各部件的作用，同时又不给网络造成过重的负担。

(4) 自动升级功能。防毒部件应具备自动更新病毒特征码数据库及其他相关信息的功能。

(5) 要害部位必须重点设防。网络服务器和文件服务器是系统的要害之一，其中保存了企业的重要数据。因此，在网络服务器和文件服务器上安装防毒软件应当是头等重要的，保证上传和下载的文件不带有病毒，对企业用户及客户的网络都是非常重要的。

2. 在网关位置设置防护软件

一般情况下，直接在网关上安装防病毒软件，可以最大限度地阻止病毒进入企业网。设置网关防护的目的是读取数据包的包头信息，进而把数据包尽快送到目的地。但如果在网关上检查病毒，就需要扫描系统接收的所有数据包，还可能要对它们进行重组，并临时存放到某个地方，以便进行病毒扫描，这样的做法存在的最大问题是会大大降低网络性能。

3. 在终端上设置防病毒软件

终端是病毒进入网络的主要途径之一，在每台终端的日常工作中进行病毒扫描，虽然性能可能略有下降，但不用增添新的设备。尽管现在不少病毒是通过文件下载或 E-mail 方式传播的，但仍有很大一部分来自人们常用的存储设备。另外，一些被压缩的软件(或数据)包中也可能有一些已被压缩的病毒，在解压时(或解压后)可能发作。因此在终端上对软件及数据做实时扫描显然是很有必要的，它可以有效降低病毒的感染机会。

9.5 Windows Server 2003 服务器安全设置

9.5.1 防火墙设置

(1) 卸载网络连接不需要的协议与服务。

在“本地连接”属性中，根据需要安装协议和服务，将不需要的协议和服务都删掉，如图 9-5 所示。在高级 TCP/IP 设置中选择“禁用 TCP/IP 上的 NetBIOS(S)”，如图 9-6 所示。

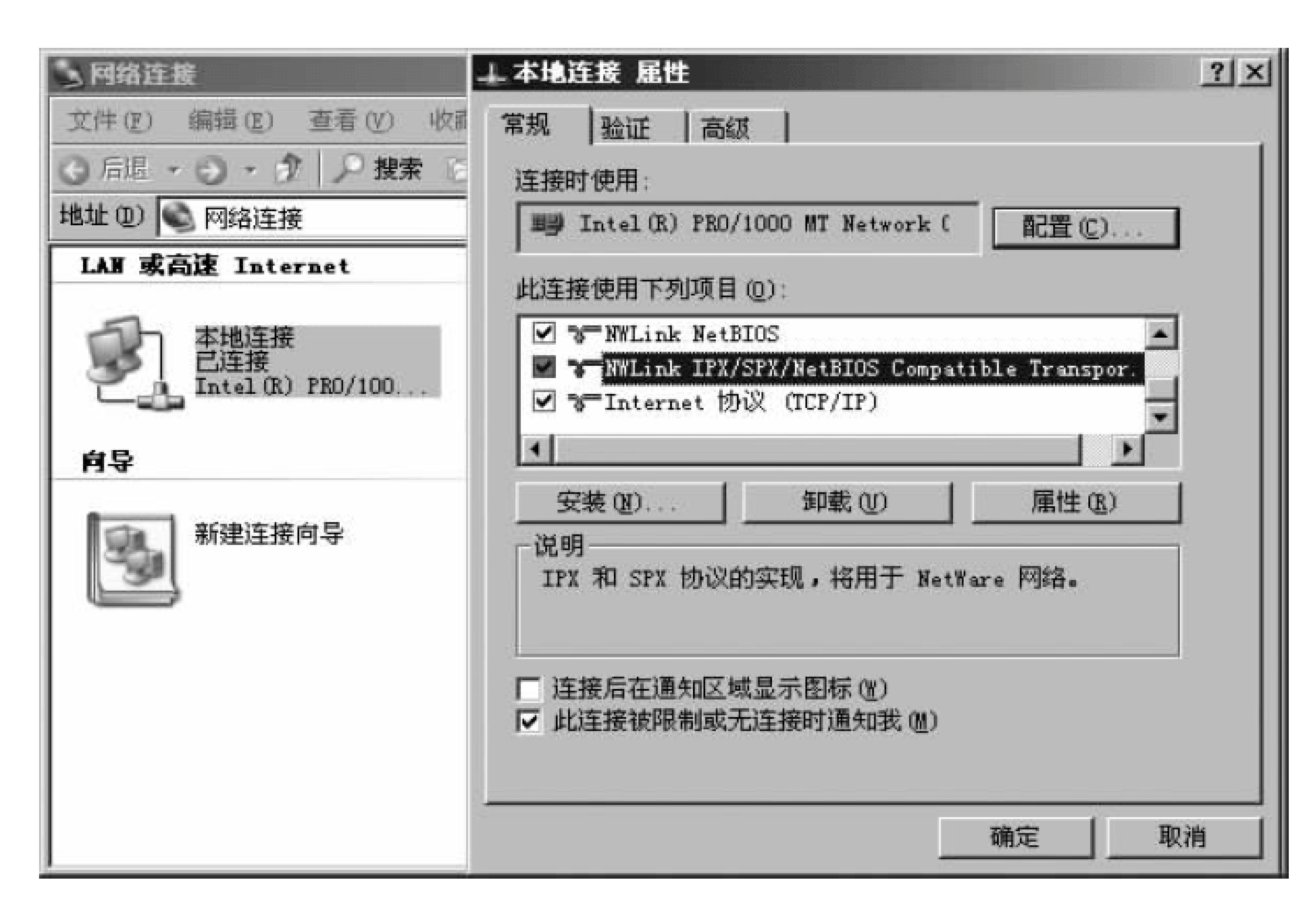


图 9-5 “本地连接”使用的协议和服务

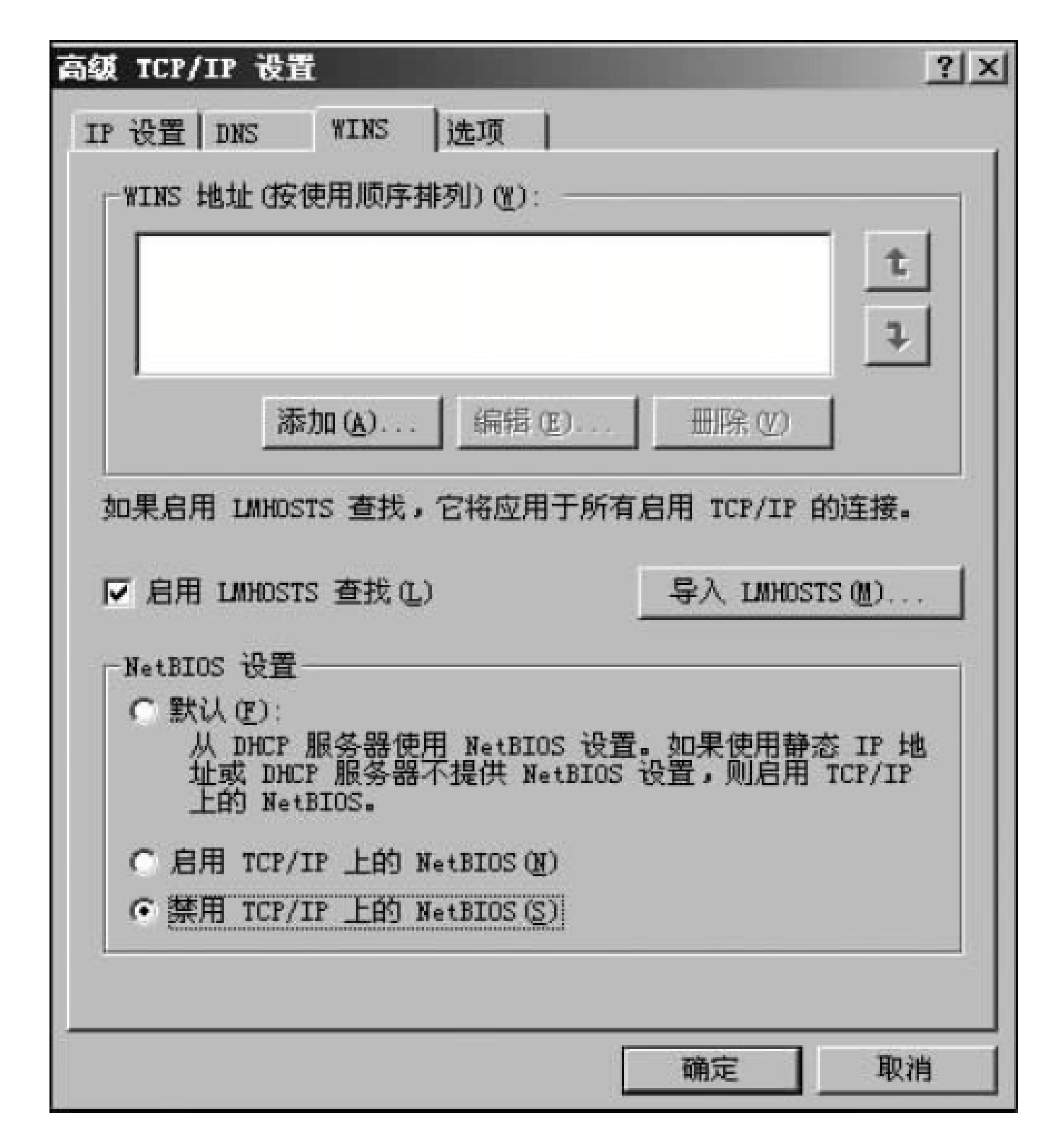


图 9-6　TCP/IP 上的 NetBIOS(S)

(2) 开启操作系统自带的防火墙。

在高级选项里，使用“Internet 连接防火墙”，这是 Windows 2003 自带的防火墙，如图 9-7 所示。



图 9-7　启动防火墙

(3) 进行系统端口管理，选择“启用 TCP/IP 筛选”复选框，如图 9-8 所示。

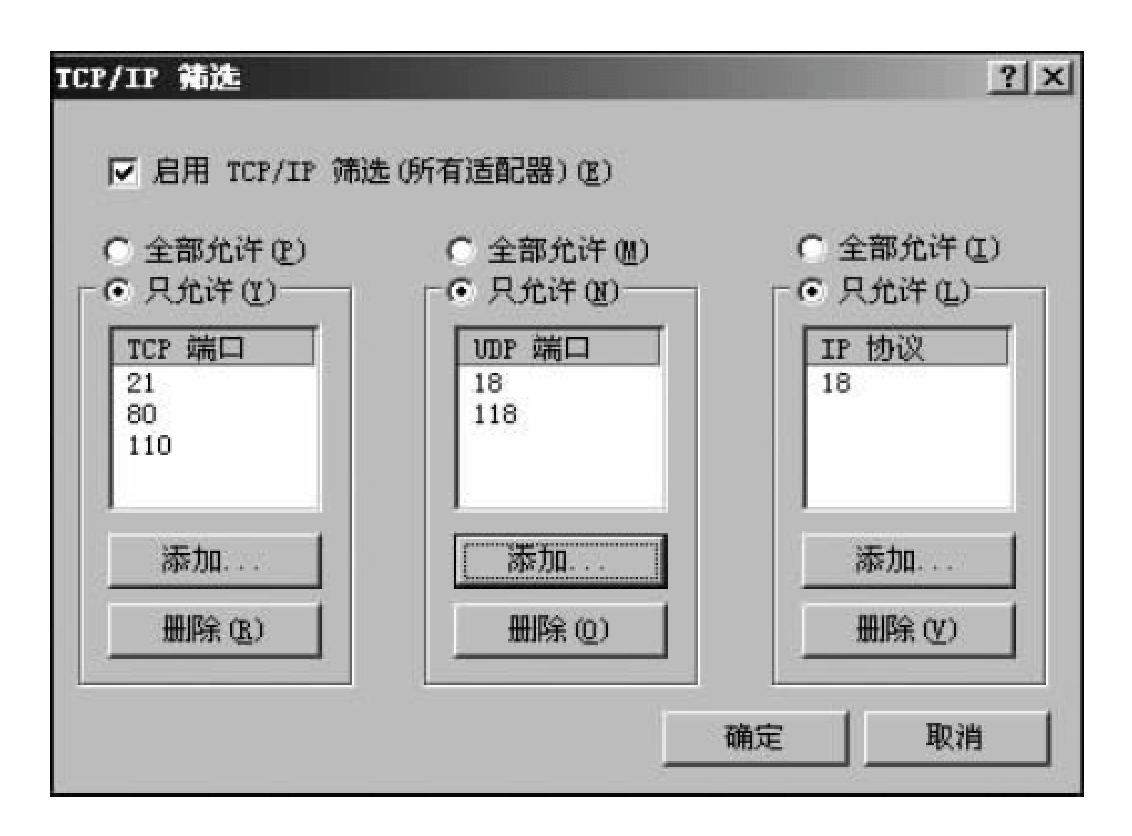


图 9-8 端口管理

9.5.2 系统权限的设置

(1) 设置磁盘权限,如图 9-9 所示。

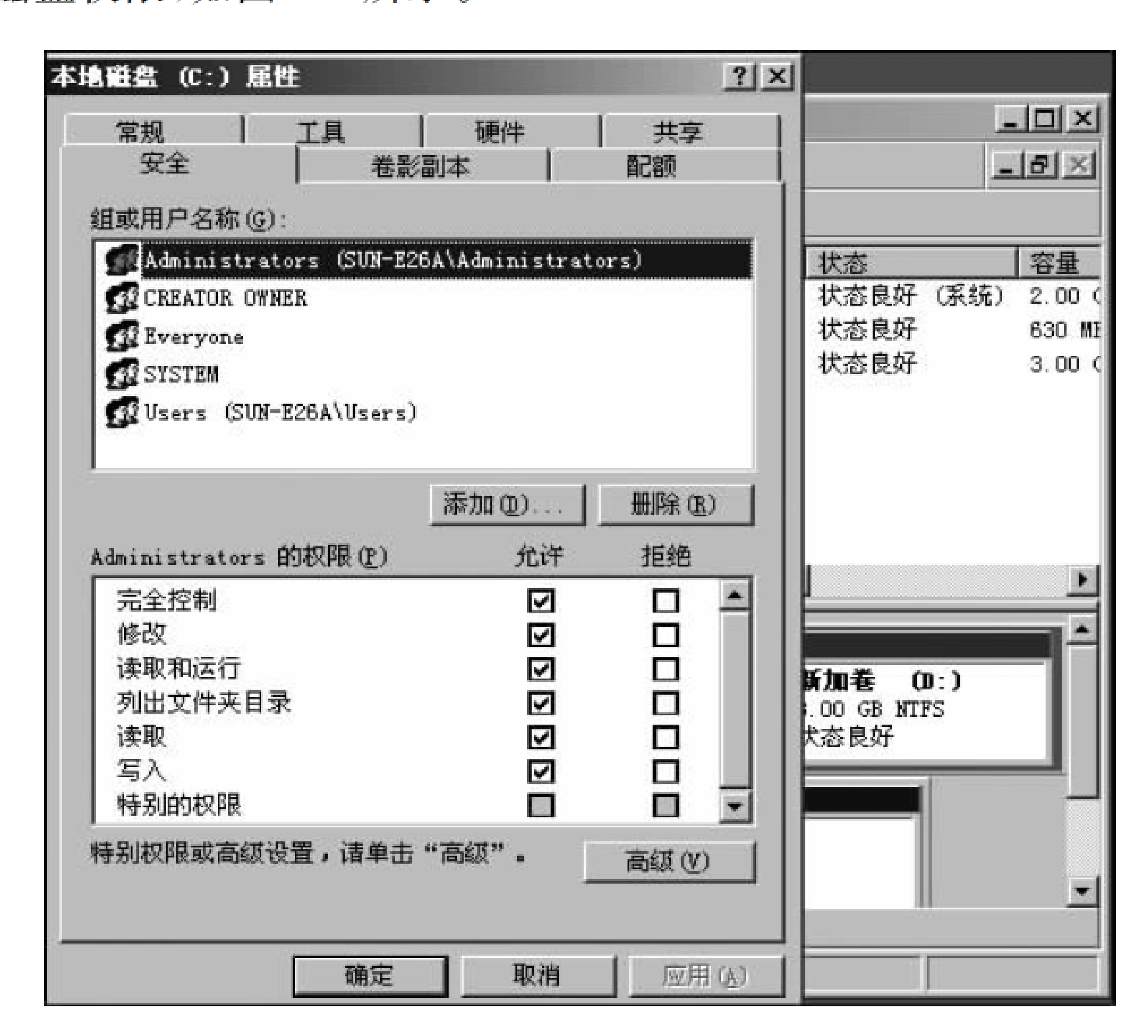


图 9-9 磁盘管理权限设置

① 系统盘及所有磁盘只给 Administrators 组和 SYSTEM 完全控制权限。

② 系统盘\Documents and Settings 目录只给 Administrators 组和 SYSTEM 完全控制权限,如图 9-10 所示。

③ 系统盘\Documents and Settings\All Users 目录,只给 Administrators 组和 SYSTEM 完全控制权限。



图 9-10　文件夹权限设置

(2) 设置文件权限。

① 系统盘\Windows\System32\cacls. exe、cmd. exe、net. exe、net1. exe、ftp. exe、tftp. exe、telnet. exe、netstat. exe、regedit. exe、at. exe、attrib. exe、format. com、del 文件只给 Administrators 组和 SYSTEM 完全控制权限。

② 另将\System32\cmd. exe、format. com 和 ftp. exe 转移到其他目录或更名。

③ Documents and Settings 下的所有目录只给 Administrators 权限。

(3) Windows Server 2003 安装完成后，删除系统盘\inetpub 目录。

9.5.3　用户权限

(1) 禁用 Guest 账号。

在计算机管理的用户选项中设置禁用 Guest 账号。

(2) 限制不必要的用户。

删除所有的 Duplicate User 用户、测试用户和共享用户等。对用户组策略设置相应权限，并且经常检查系统的用户，删除已经不再使用的用户。

(3) 将系统 Administrator 账号改名。

Windows 2003 的 Administrator 用户是不能被停用的，这意味着入侵者可以一遍又一遍地尝试这个用户的密码。可以把它伪装成普通用户，比如改成 Great wall。

(4) 创建一个陷阱用户。

所谓陷阱用户，就是创建一个名为 Administrator 的本地用户，降低它的权限，并且加上复杂的密码，给入侵者增加困难。图 9-11 中的 Administrator 已经不是管理员，而是陷阱用户。



图 9-11 用户权限设置

(5) 把共享文件的权限从 Everyone 组改成授权用户。

任何时候都不要把共享文件的用户设置成 Everyone 组,包括打印共享。默认的属性就是 Everyone 组的用户拥有共享权限。

9.5.4 策略设置

选择"控制面板"→"管理工具"→"本地安全策略",打开"本地安全策略"窗口,在其中进行安全策略的设置。

(1) 设置密码策略。充分应用密码策略,如启用密码复杂性要求,设置密码长度最小值为 10 位,设置强制密码,用记事本记录密码,定期或不定期地更换密码。

(2) 设置账户锁定策略。分别设置复位用户锁定计数器时间、用户锁定时间和用户锁定阈值,如图 9-12 所示。



图 9-12 账户锁定策略

(3) 设置合理的审核策略,如图 9-13 所示。

(4) 设置用户权限分配。仔细核实各项策略中的用户权限分配情况,清除不必要的用户。

例如,关闭系统的权限只授予 Administrators 组,将其他组或用户全部删除。

(5) 设置安全选项。逐项检查安全选项设置,清除不必要的策略选项。



图 9-13 审核策略

例如，逐项检查以下针对网络访问的安全选项策略。

网络访问：启用不允许 SAM 账户和共享的匿名枚举。

网络访问：启用不允许为网络身份验证储存凭证。

网络访问：全部删除可匿名访问的共享。

网络访问：全部删除可匿名访问的命名。

网络访问：全部删除可远程访问的注册表路径。

网络访问：全部删除可远程访问的注册表路径和子路径。

9.5.5 IP 安全策略

(1) 需要封闭如下端口。

TCP：135,137,138,139,445,593,1025,2745,3127,3128,6129。

UDP：135、137、138、139、445。

(2) 创建 IP 安全策略。选中“IP 安全策略，在本地计算机”，在右边窗体的空白位置右击，在弹出的快捷菜单中选择“创建 IP 安全策略”命令，在弹出的“IP 安全策略向导”的对话框中单击“下一步”按钮，为新的安全策略命名，如图 9-14 所示。再单击“下一步”按

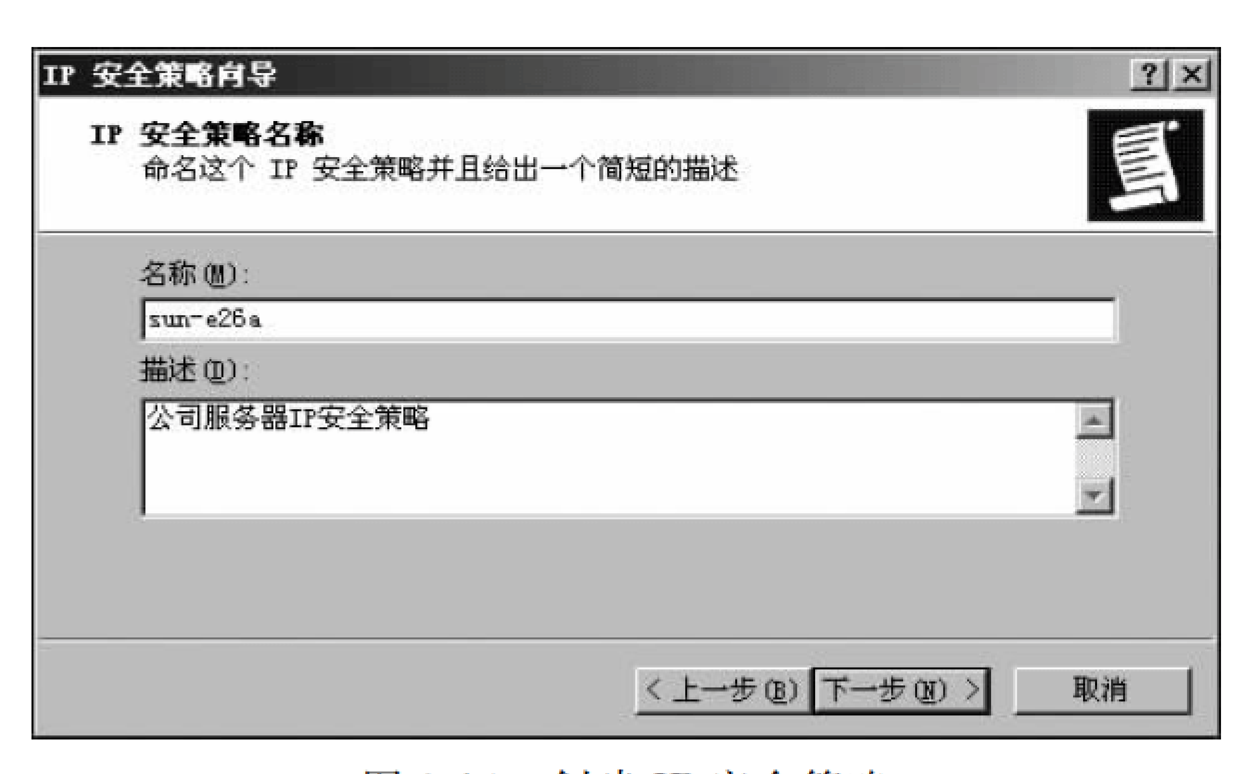


图 9-14 创建 IP 安全策略

钮，则显示“安全通信请求”对话框，在其中把“激活默认相应规则”复选框的钩去掉，单击“完成”按钮，就创建了一个新的 IP 安全策略。

(3) 添加新的 IP 筛选器。右击该 IP 安全策略，在“属性”对话框中，把“使用添加向导”复选框的钩去掉，然后单击“添加”按钮添加新的规则，随后弹出“新规则属性”对话框，在其中单击“添加”按钮，弹出 IP 筛选器列表窗口，在列表中，首先把“使用添加向导”复选框的钩去掉，然后再单击右边的“添加”按钮添加新的筛选器。

(4) 添加屏蔽 IP 地址。进入“筛选器属性”对话框，在“地址”选项卡中，源地址选“任何 IP 地址”，目标地址选“我的 IP 地址”。选择“协议”选项卡，在“选择协议类型”的下拉列表中选择 TCP，然后在“到此端口”下的文本框中输入 135，单击“确定”按钮(如图 9-15 和图 9-16 所示)，这样就添加了一个屏蔽 TCP 135(RPC)端口的筛选器，它可以防止外界通过 135 端口连上用户的计算机。



图 9-15 地址选择



图 9-16 端口筛选

(5) 在“本地安全策略”窗口中，右击新添加的 IP 安全策略，在快捷菜单中选择“指派”命令。

9.5.6 修改注册表

选择“开始”→“运行”，在运行对话框中输入 regedit 并按回车键，打开注册表。

(1) 关闭 445 端口。在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\netBT\Parameters 中，新建“DWORD 值”，值名为 SMBDeviceEnabled，数据为默认值 0。

(2) 禁止建立空连接。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 中，新建“DWORD 值”，值名为 RestrictAnonymous，数值为 1。

(3) 禁止系统自动启动服务器共享。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 中，新建“DWORD 值”，值名为 AutoShareServer，数值为 0。

(4) 禁止系统自动启动管理共享。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters 中，新建“DWORD 值”，值名为 AutoShareWks，数值为 0。

(5) 禁止响应 ICMP 路由通告报文。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface 中，新建 DWORD 值，值名为 PerformRouterDiscovery，数值为 0。

(6) 防止 ICMP 重定向报文的攻击。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 中，修改 EnableICMPRedirects 的数值为 0。

(7) 不支持 IGMP 协议。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 中，新建 DWORD 值，值名为 IGMPLevel，数值为 0。

(8) 防止小规模 DDOS 攻击。在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 中，新建“DWORD 值”，值名为 SynAttackProtect，数值为 1。

(9) 更改 TTL 值。入侵者可以根据 ping 命令返回的 TTL 值来大致判断用户的操作系统，例如：

```
TTL=107          (系统为 Windows NT)
TTL=128          (系统为 Windows 2003)
TTL=127 或 128   (系统为 Windows 9x)
TTL=240 或 241   (系统为 Linux)
```

实际上用户可以自己修改 TIL 值，在 HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\Services\Tcpip\Parameters 中，将 Default TTL REG_DWORD 0～0xff(十进制 0～255，默认值为 128)中的数值改成一个无意义的数字，如 200，对入侵者有一定的迷惑作用。

9.5.7 IIS 站点设置

(1) 将 IIS 目录的数据与系统磁盘分开，保存在专用磁盘空间内。

(2) 启用父级路径。

(3) 在 IIS 管理器中删除所有没有用到的或不必要的映射。

(4) 在 IIS 中将 HTTP 404 Object Not Found 出错页面通过 URL 重定向到一个定制 HTM 文件，如图 9-17 所示。



图 9-17 HTTP 404 页面重定向

(5) Web 站点权限设定。

建议取消“索引资源”复选框勾选，并且“与执行权限”不选择“脚本和可执行文件”，如图 9-18 所示。

(6) 建议使用 W3C 扩充日志文件格



图 9-18　Web 站点权限设定

式,每天记录客户 IP 地址、用户名、服务器端口、方法、URI 字根、HTTP 状态和用户代理,而且每天均要审查日志,如图 9-19 所示。

建议不要使用默认的目录,更换一个日志的路径,同时设置日志的访问权限,只允许管理员和 system 拥有完全控制权限,如图 9-20 所示。



图 9-19　日志路径



图 9-20　日志属性

(7) 程序安全设定。

① 涉及用户名与口令的程序最好封装在服务器端,尽量少的在 ASP 文件里出现,涉及与数据库连接地用户名与口令应给予最小的权限。

② 需要经过验证的 ASP 页面,可跟踪上一个页面的文件名,只有从上一页面转进来的会话才能读取这个页面。

③ 防止 ASP 主页.inc 文件泄露问题。

(8) IIS 权限设置的思路。

为每个独立需要保护的对象(比如一个网站或者一个虚拟目录)创建一个系统用户，让这个站点在系统中具有唯一的可以设置权限的身份，如图 9-21 所示。

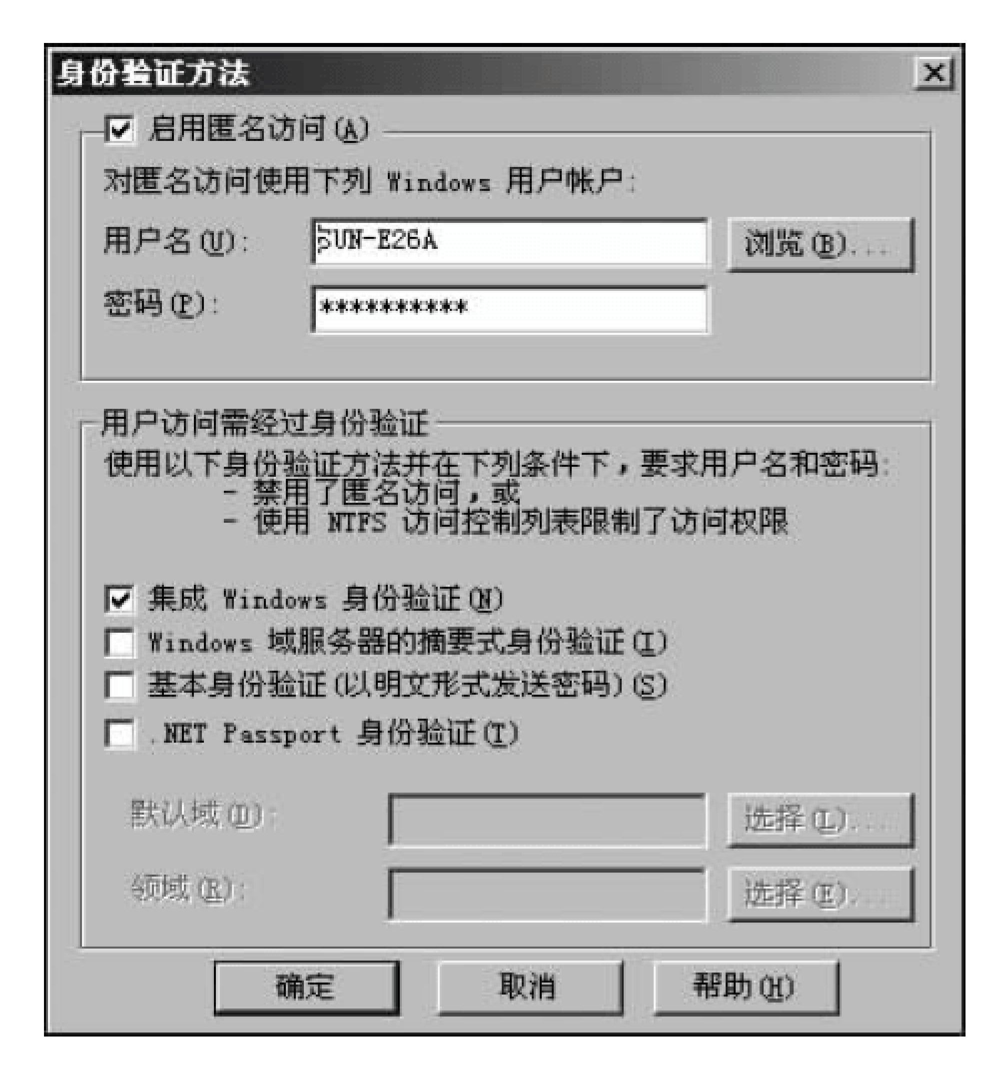


图 9-21 设置站点权限

(9) 特殊站点服务也可以启动证书服务器。

Windows Server 2003 系统中的证书服务器用于向 Web 站点发放证书，默认情况下系统没有安装证书服务器，因此需要进行手动安装。

9.5.8 其他安全设置

(1) 建立一个记事本，输入以下代码。保存为.bat 文件并加到启动项目中，删除未知共享。

```
@echo off
net share c$ /del
net share d$ /del
net share e$ /del
net share f$ /del
net share ipc$ /del
net share admin$ /del
```

(2) 禁用不必要的服务。

选择“开始”→“运行”，在“运行”对话框中输入 Services.msc 并按回车键，出现“服务”窗口，列出了所有本地服务。

以下是 Windows Server 2003 系统默认禁用的服务项，如果没有特别需要不要启动。

Server：支持此计算机通过网络的文件、打印和命名管道共享。

Computer Browser：维护网络上计算机的最新列表以及提供这个列表。

Task Scheduler：允许程序在指定时间运行。

Messenger：传输客户端和服务器之间的 NET SEND 和警报器服务消息。

Distributed File System：局域网管理共享文件，不需要时可禁用。

Distributed Link Tracking Client：用于局域网更新连接信息，不需要时可禁用。

Error Reporting Service：禁止发送错误报告。

Microsoft Search：提供快速的单词搜索，不需要时可禁用。

NTLM Security Support Provide：Telnet 服务和 Microsoft Search 使用的服务，不需要时可禁用。

Print Spooler：如果没有打印机则可禁用。

Remote Registry：远程修改注册表，应禁用。

Remote Desktop Help Session Manager：远程协助，应禁用。

Workstation：若关闭此项服务，远程 NET 命令列不出用户组。

9.6 本章小结

以 Internet 为代表的计算机网络应用得到了飞速发展。作为 Internet 的协议基础的 TCP/IP 协议族具有开放性和方便性等优点。由于 TCP/IP 在设计上的安全性缺陷，在 Internet 高速发展的今天，网络安全与网络管理面临更大的挑战。

网络安全是为保障网络服务的可用性、网络信息的完整性以及可靠性不被蓄意或偶然地破坏而采取的一切措施。网络安全研究是当今网络研究的一个热点，也是当今网络应用中最敏感的问题之一。

随着网络技术的发展和网络应用的更加普及，新的网络安全问题又会出现。目前尚未出现任何能够一劳永逸的网络安全解决方案。研究网络安全分析、网络安全策略管理和网络安全技术的目的就是用尽可能少的代价把风险降到最低。

综合训练

一、理论题

1. 选择题

(1) 计算机网络的安全是指(　　)。

A. 计算机中设备设置环境的安全　　B. 网络使用者的安全

C. 网络中信息的安全　　D. 网络中财产的安全

(2) 信息不泄露给非授权用户、实体或过程或供其利用的特性即网络安全特性中的(　　)。

A. 保密性　　B. 完整性　　C. 可用性　　D. 不可否认性

(3) 防火墙只能抵御来自(　　)的侵扰,而对企业内部网络的安全却无能为力。

A. 外部网络　　B. 应用系统　　C. 外部网络　　D. 操作系统

(4) 信息加密过程是由许多复杂(　　)的来具体实施的。

A. 安全策略　　B. 防火墙　　C. 加密算法　　D. 杀毒软件

2. 填空题

(1) 计算机网络隐患包括________、________、________、________和________等。

(2) 安全入侵从其利用的漏洞上可以大致分为下面 3 种:________、________和________。

(3) 网络安全的基本要素是________、________、________、________和________、________。

(4) 用户安全可以采用以下保护:________、________和________、________、________等。

3. 简答题

(1) 计算机网络安全涉及的内容有哪些?

(2) 简述网络安全策略。

二、实践题

1. Telnet 入侵防范设置

Telnet 协议是 TCP/IP 协议族中的一员,是 Internet 远程登录服务的主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。Telnet 是常用的远程控制 Web 服务器的方法。Telnet 可能是黑客常用的攻击方式,用户可以通过修改 Telnet 服务端口或者停用 Telnet 服务来防范 Telnet 入侵。

参考步骤如下:

(1) 打开“计算机管理”,单击“服务”。

(2) 找到“Telnet 服务”,右击该项,在快捷菜单中选择“属性”命令,停用 Telnet 服务。

2. 网页恶意代码的防范措施

参考步骤如下:

(1) 运行 IE 时,选择“工具”→“Internet 选项”,在“Internet 属性”窗口中选择“安全”选项卡,在“该区域的安全级别”下把安全级别由“中”改为“高”,如图 9-22 所示。

(2) 网页恶意代码主要是含有恶意代码的 ActiveX 或 Applet、JavaScript 的网页文件,所以在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止,可以减少被网页恶意



图 9-22 设置 Internet 安全级别

代码感染的几率。

具体操作如下：在 IE 窗口中选择“工具”→“Internet 选项”，在弹出的对话框中选择“安全”选项卡，再单击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有 ActiveX 插件和控件以及与 Java 相关的全部选项都设为“禁用”，如图 9-23 所示。



图 9-23 Internet 安全设置

第10章　网络安全管理工具软件应用

本章主要内容

- X-Scan 安全漏洞扫描器
- Wireshark 网络数据包分析软件
- 天网防火墙设置
- 超级扫描工具 SuperScan
- 网络侦测工具 Essential NetTools
- 超级网管 SuperLANadmin
- 流量分析器 CommView
- Simple Server Monitor 服务监控

在日常网络安全管理工作中,借助网络工具可以达到事半功倍的效果。网络是一个复杂的体系,并且在不断变化之中,网络安全管理是一件非常烦琐的工作,为了网管人员的工作方便,本章集中介绍从网络安全探测到网络安全配置的网管工具,包括 X-Scan 安全漏洞扫描器、超级网管 SuperLANadmin 等 8 个网管工具。

10.1　系统扫描器

10.1.1　功能简介

扫描器的定义比较广泛,不限于一般的端口扫描,也不限于针对漏洞的扫描,可以是对某种服务或某个协议的扫描。然而,端口扫描是扫描系统中最基本的形态和模块。扫描器的主要功能如下:

(1) 检测主机是否在线。

(2) 扫描目标系统开放的端口,有的还可以测试端口的服务信息。

(3) 获取目标操作系统的敏感信息。

(4) 破解系统口令。

(5) 扫描其他系统敏感信息。

一个优秀的扫描器能检测整个系统各个部分的安全性,能获取各种敏感的信息,并能试图通过攻击以观察系统反应等。

10.1.2　X-Scan 应用

X-Scan 可以快速地扫描指定计算机存在的安全漏洞,以及快速地了解安全漏洞的处

理方法。该工具的优点是可以较全面地扫描漏洞，缺点是扫描大范围网络时会占用大量的系统资源。

（1）X-Scan 运行后的主界面如图 10-1 所示。

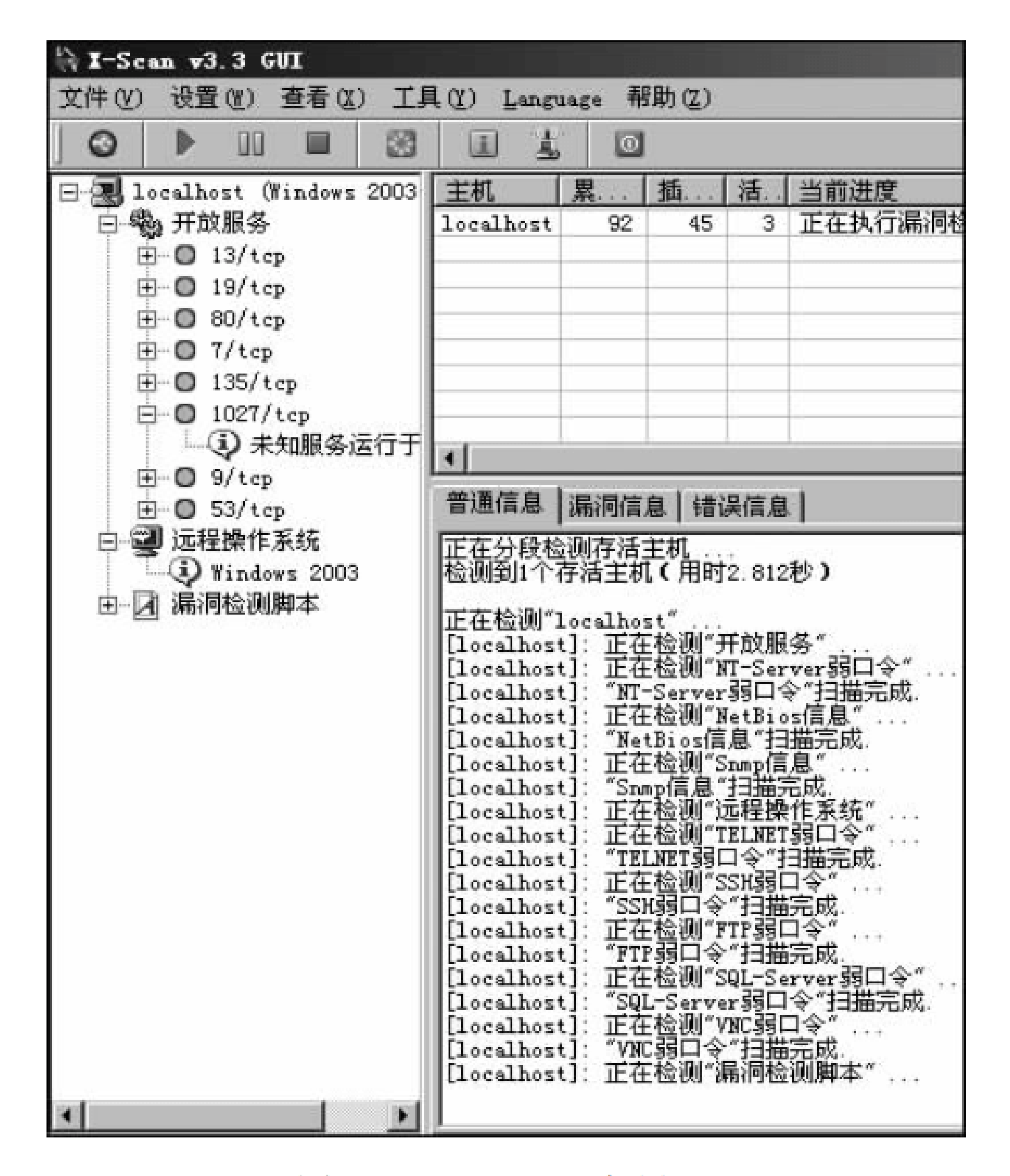


图 10-1　X-Scan 主界面

（2）扫描主机后，X-Scan 列出端口/协议漏洞清单，如图 10-2 所示。

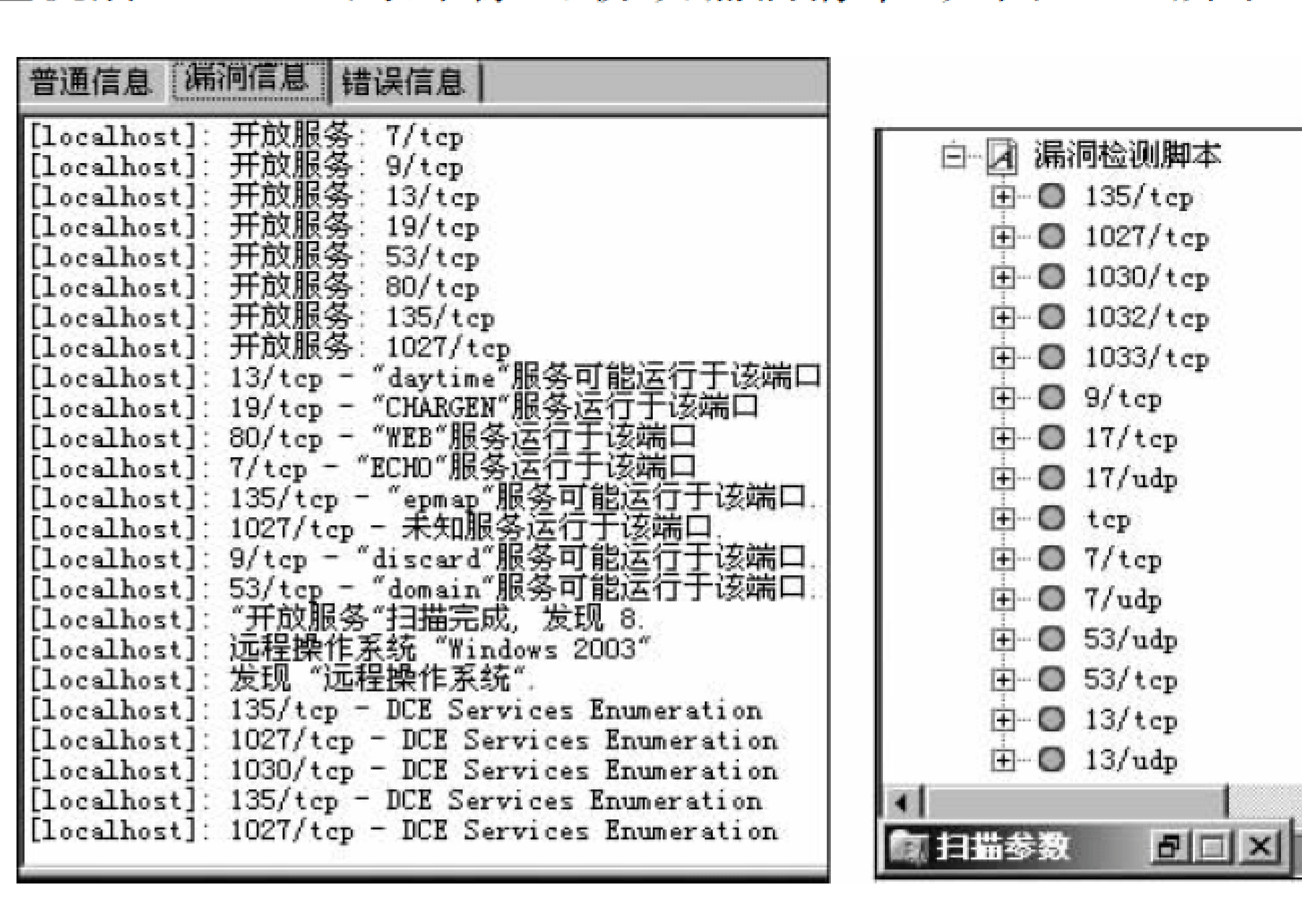


图 10-2　漏洞清单

（3）X-Scan 工具扫描主机后，提供检测报告，文件格式为 HTML，如图 10-3 所示。

（4）扫描端口报告，如图 10-4 所示。

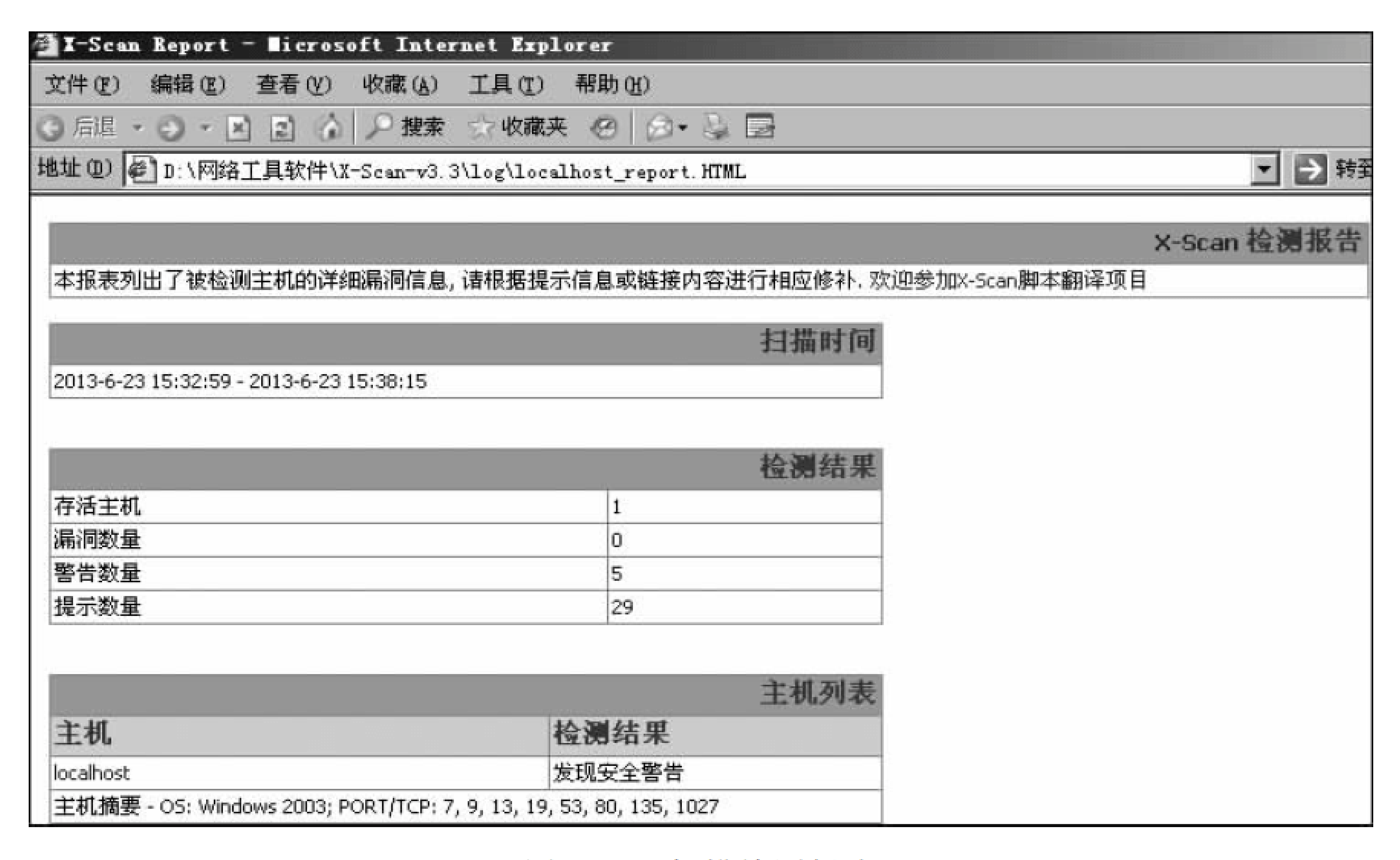


图 10-3　扫描检测报告

主机分析: localhost		
主机地址	**端口/服务**	**服务漏洞**
localhost	daytime (13/tcp)	发现安全提示
localhost	chargen (19/tcp)	发现安全提示
localhost	www (80/tcp)	发现安全提示
localhost	echo (7/tcp)	发现安全警告
localhost	epmap (135/tcp)	发现安全提示
localhost	unknown (1027/tcp)	发现安全提示
localhost	discard (9/tcp)	发现安全警告
localhost	domain (53/tcp)	发现安全提示
localhost	DCE/50abc2a4-574d-40b3-9d66-ee4fd5fba076 (1027/tcp)	发现安全提示
localhost	DCE/12345778-1234-abcd-ef00-0123456789ac (1030/tcp)	发现安全提示
localhost	DCE/45f52c28-7f9f-101a-b52b-08002b2efabe (1032/tcp)	发现安全提示
localhost	unknown (1033/tcp)	发现安全提示
localhost	DCE/811109bf-a4e1-11d1-ab54-00a0c91e9b45 (1032/tcp)	发现安全提示
localhost	BBN IAD (1032/tcp)	发现安全提示
localhost	DCE/6bffd098-a112-3610-9833-46c3f874532d (1033/tcp)	发现安全提示
localhost	DCE/5b821720-f63b-11d0-aad2-00c04fc324db (1033/tcp)	发现安全提示

图 10-4　扫描端口报告

(5) X-Scan 软件提供漏洞扫描解决方案，在实际应用中，需要网络管理人员逐项认真阅读并加以处理，这里只截取了解决方案的一部分，如图 10-5 所示。

用户应根据实际情况，参照 X-Scan 工具提供的安全漏洞解决方案，进行主机安全设置与安全策略管理。

安全漏洞及解决方案: localhost

类型	端口/服务	安全漏洞及解决方案
提示	daytime (13/tcp)	**开放服务** "daytime"服务可能运行于该端口. BANNER信息: 31 35 3a 33 33 3a 31 32 20 32 30 31 33 2d 36 2d 15:33:12 2013-6- 32 33 0a 23 NESSUS_ID : 10330
提示	daytime (13/tcp)	**Daytime** The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host. In addition to that, the UDP version of daytime is running, an attacker may link it to the echo port of a third party host using spoofing, thus creating a possible denial of service condition between this host and

图 10-5　解决方案

10.2　网络监听

10.2.1　功能简介

网络监听是黑客在网络中常用的一种技术，通过网络中监听其他人的数据包，分析数据包，从而获得一些敏感信息，如账号和密码等。网络监听原本是网络管理员经常使用的一个工具，主要用来监视网络的流量、状态和数据等信息。另外，分析数据包对于防范黑客入侵有比较重要的意义，通过深入了解扫描过程、攻击方式等，从而为防火墙制定相应的防范规则。

10.2.2　使用 Wireshark 捕捉数据报

Wireshark 是一个网络数据包分析软件。网络数据包分析软件的功能是抓取网络数据包，并尽可能地显示出最为详细的网络封包资料。

（1）Wireshark 网络包分析工具的主要作用是在接口实时捕捉网络包，并显示包的详细协议信息。Wireshark 可以捕捉多种网络接口类型（包括无线局域网接口）的包，如图 10-6 所示。Wireshark 可以打开多种网络分析软件捕捉的包，可以支持许多协议的解码。可以用它来检测网络安全隐患，解决网络问题，也可以用它来学习网络协议以及测试协议执行情况等。

（2）过滤任务配置，如图 10-7 所示。

设置捕获缓存大小（Buffer）：设置写入数据到磁盘前保留在核心缓存中的捕获数据的大小。如果发现丢包，可尝试增大该值。

设置网卡是否为混杂捕获模式（Use promiscuous mode on all interfaces）：指定

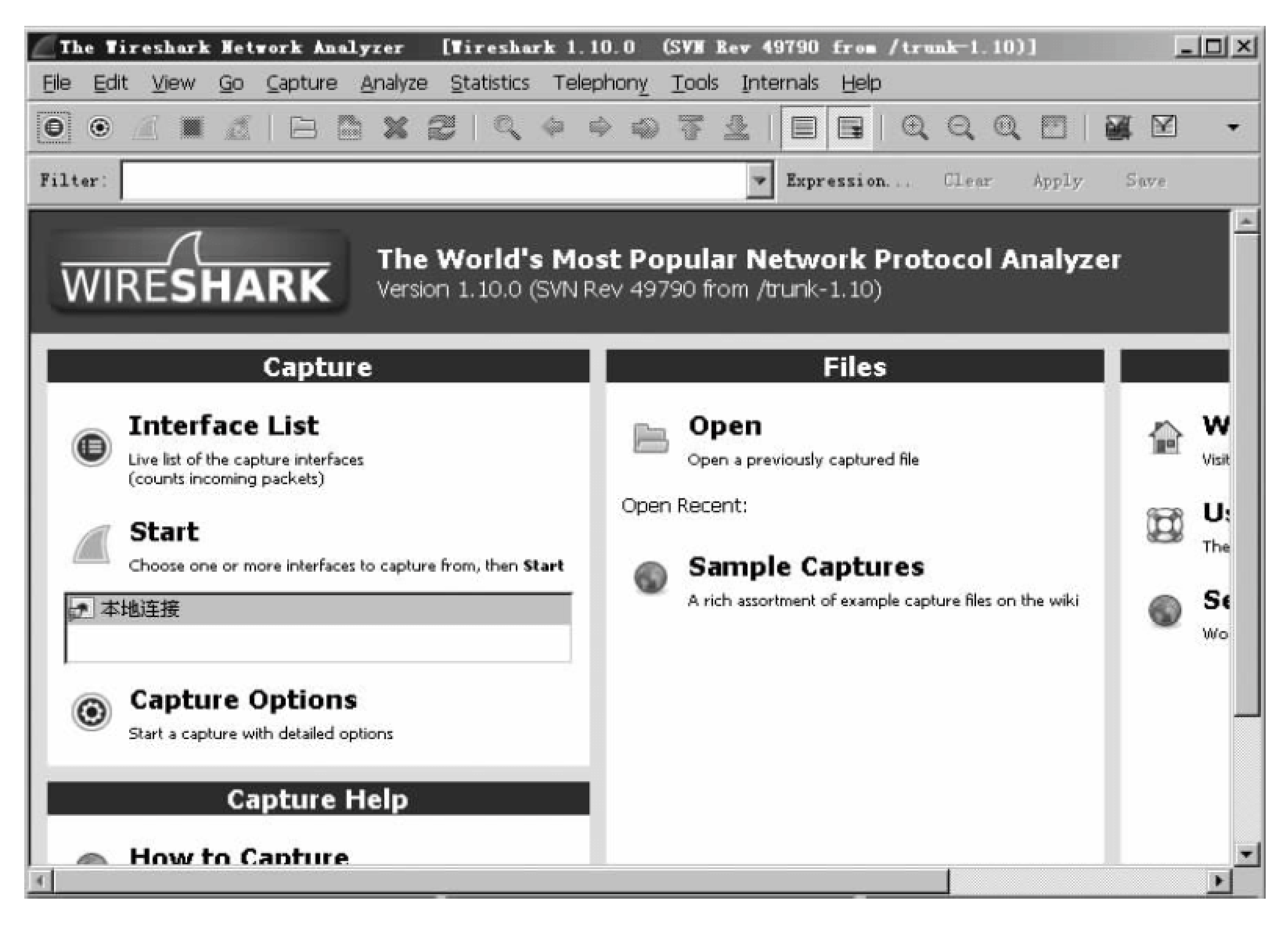


图 10-6　Wireshark 主界面

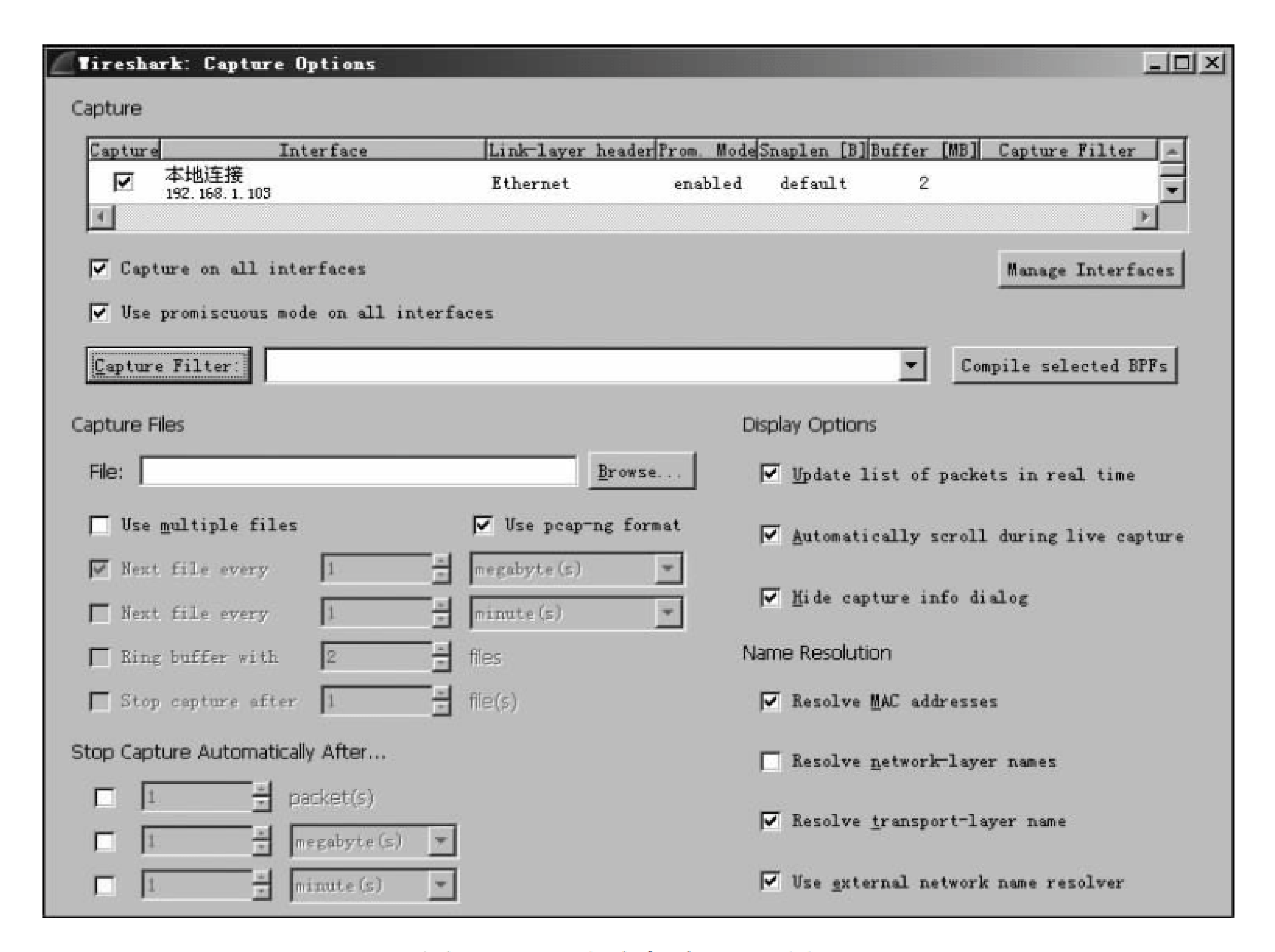


图 10-7　过滤任务配置界面

Wireshark 捕捉包时是否将接口设置为混杂接收模式。

在非混杂模式下，Wireshark 捕获满足以下条件的包：本网卡地址单播包、具有多播地址且与本网卡地址配置相吻合的数据包、广播包。而在混杂模式下，Wireshark 除捕获上述类型的数据包外，与本网卡地址配置不吻合的组播包也会被捕获下来。

设置捕获过滤规则：Wireshark 使用 libpcap 过滤语句进行捕捉过滤。

(3) 查看当前 Ethernet 接口卡信息，如图 10-8 所示。

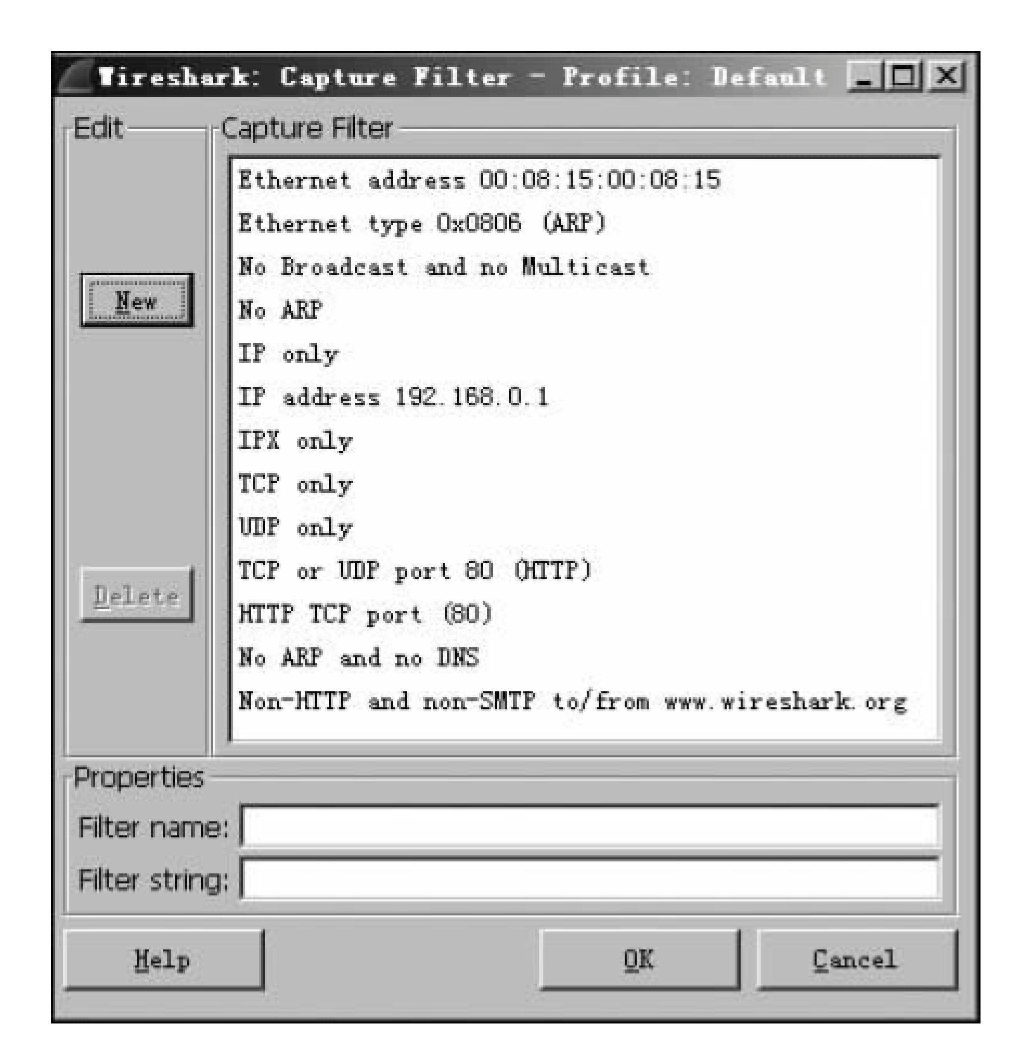


图 10-8　当前 Ethernet 接口卡信息

(4) 包分析主窗体，如图 10-9 所示。

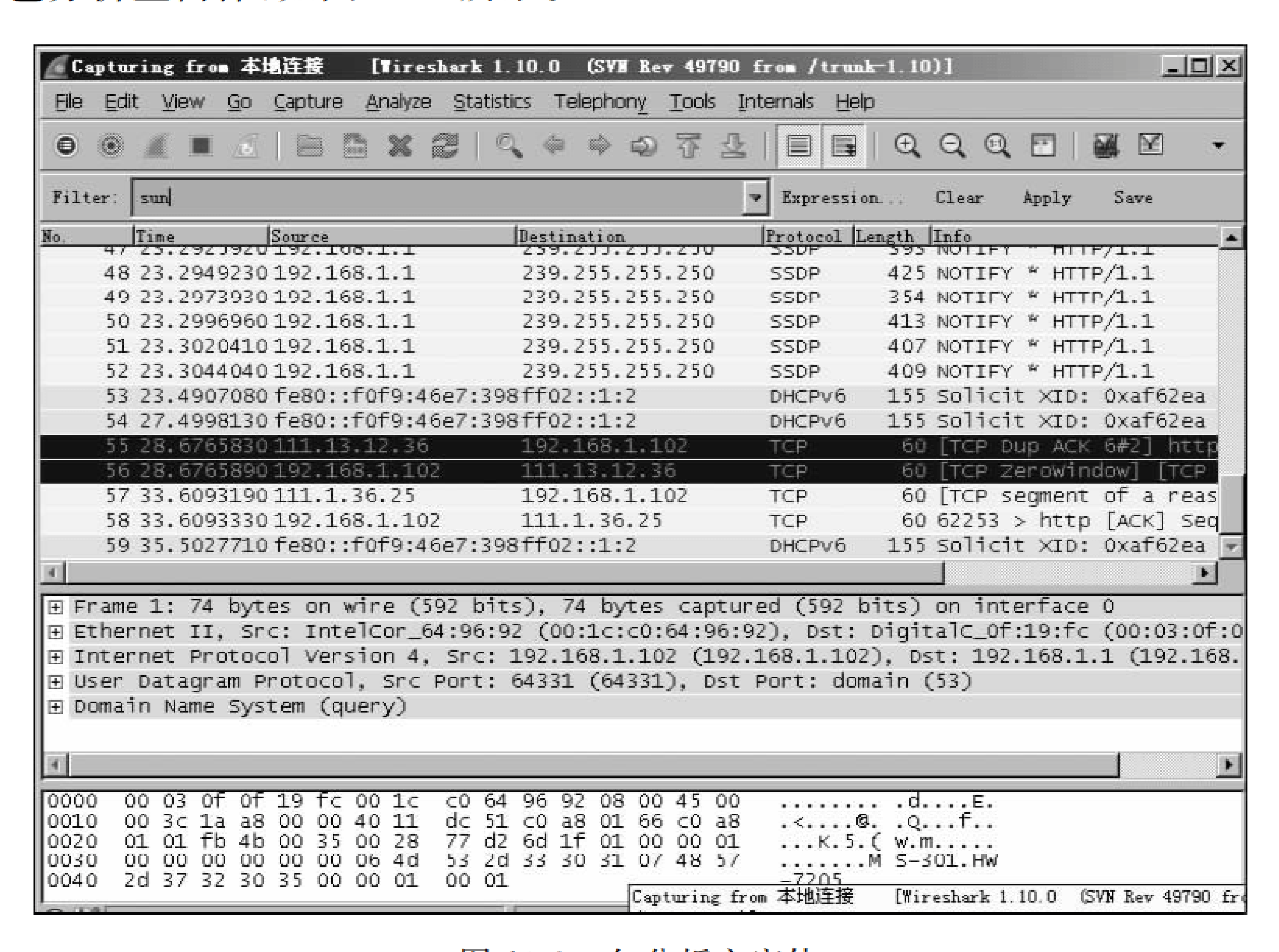


图 10-9　包分析主窗体

包分析主窗体包括 3 个窗格：包信息概况窗格、协议信息窗格和数据信息显示窗格，三者同时反映包信息属性。

(5) 浏览显示内容，可以隐藏一些不感兴趣的包，将注意力集中在感兴趣的那些包上

面，如图 10-10 所示。

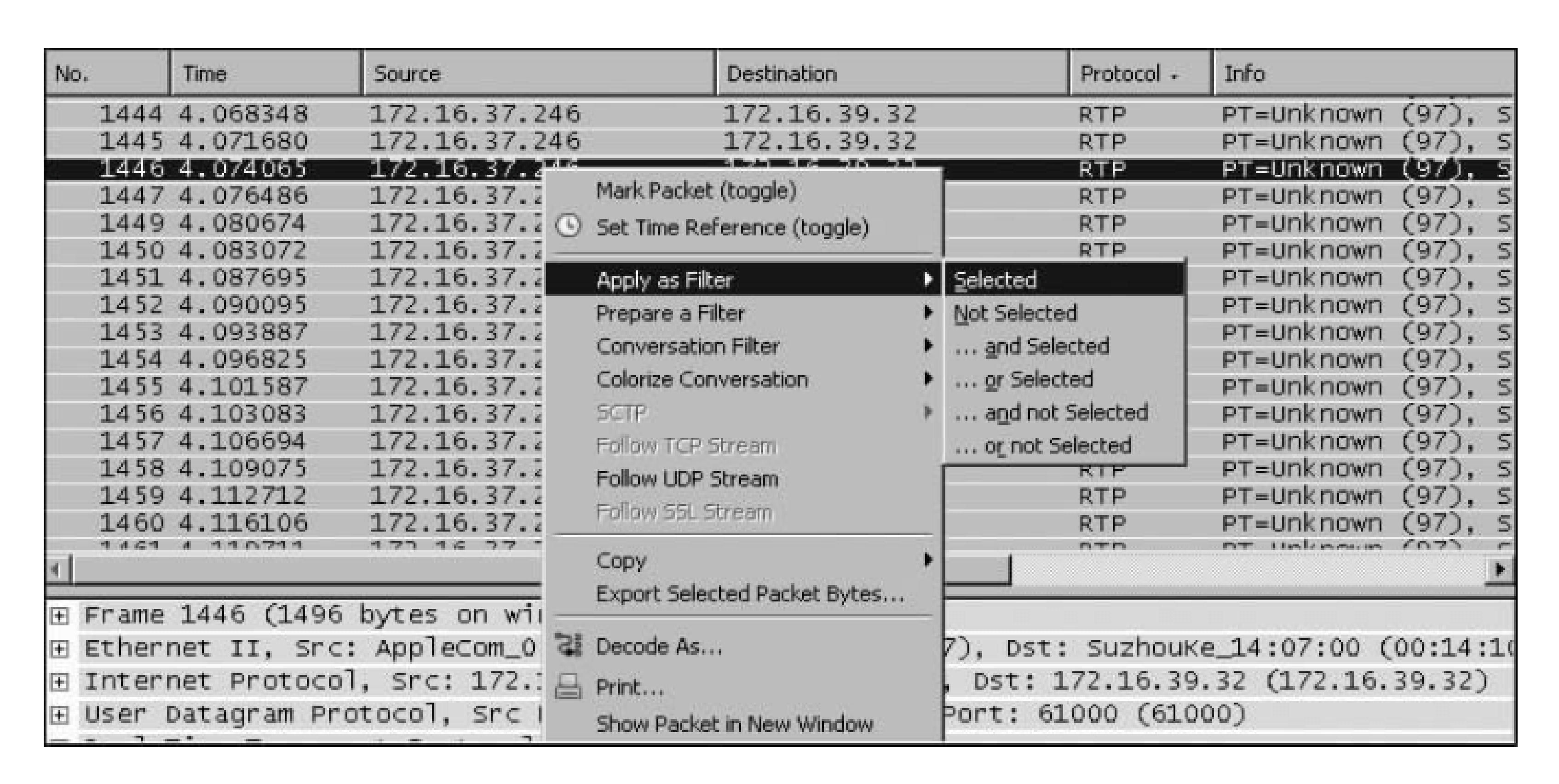


图 10-10　浏览过滤包

（6）会话统计，即对两个特定端点之间发生的通信进行统计，如图 10-11 所示。

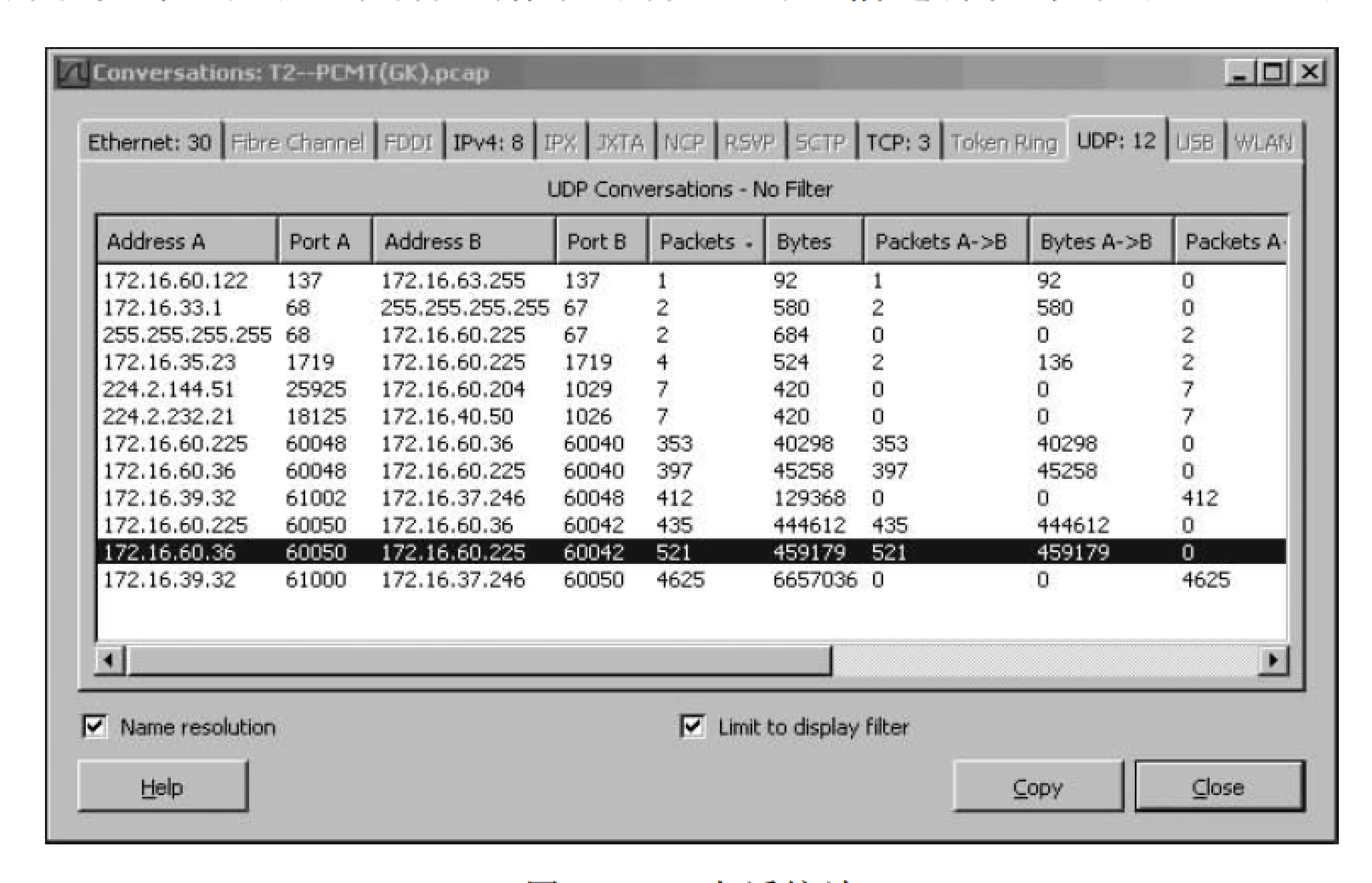


图 10-11　会话统计

Wireshark 网络数据包分析软件功能十分强大，对其感兴趣的读者可以查阅更加详细的资料。

10.3　防火墙应用

10.3.1　功能简介

防火墙是一种高级访问控制设备，置于不同网络安全域之间，它通过相关的安全策略来控制允许/拒绝进出网络，并监视、记录访问行为。

防火墙的核心技术包括以下几个方面。

(1) 包过滤是最常用的技术。包过滤技术工作在网络层，根据数据包头中的 IP、端口和协议等确定是否让数据包通过。

(2) 应用代理是另一种主要技术。应用代理工作在第 7 层——应用层，通过编写应用代理程序，实现对应用层数据的检测和分析。

(3) 状态检测。状态检测技术工作在 2～4 层，控制方式与包过滤技术相同，但处理的对象不是单个数据包，而是整个连接。状态检测通过管理人员和网络使用人员事先设定的规则表和连接状态表，综合判断是否允许数据包通过。

(4) 完全内容检测。完全检测需要很强的性能支撑，它既有包过滤功能，也有应用代理的功能。该技术工作在 2～7 层，不仅分析数据包头信息和状态信息，而且对应用层协议进行还原和内容分析，有效防范混合型安全威胁等。

10.3.2 天网个人防火墙设置

(1) 运行防火墙设置向导，根据向导进行基本设置，如图 10-12 所示。

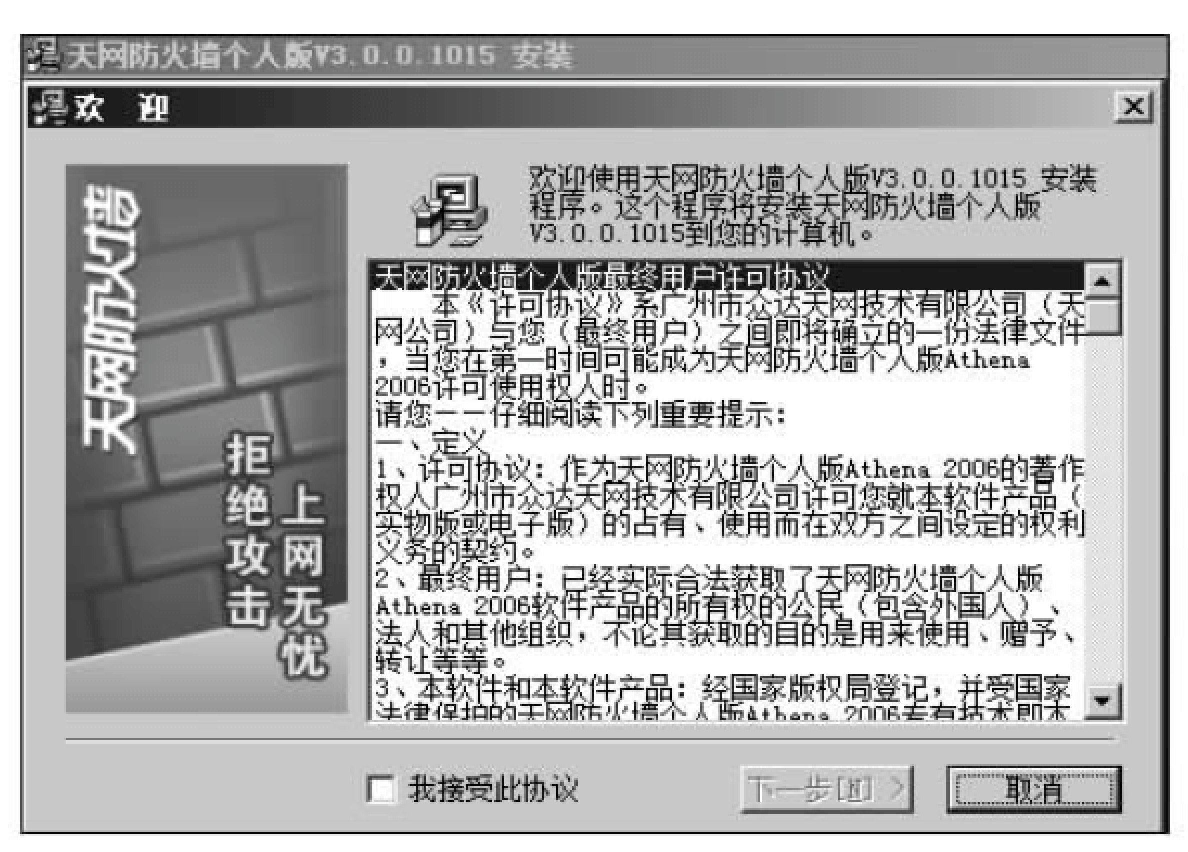




图 10-12　设置向导

(2)设置防火墙启动规则与主机 IP 地址,如图 10-13 所示。



图 10-13 设置启动规则和主机 IP

(3)允许穿越防火墙的常用应用程序设置,如图 10-14 所示。



图 10-14 常用应用程序设置

（4）防火墙安装完成，如图 10-15 所示。



图 10-15　安装完毕

（5）重新启动计算机，进行防火墙设置，选择安全级别，如图 10-16 所示。



图 10-16　防火墙设置

（6）针对常用应用程序的网络连接请求，设置防火墙规则，如图 10-17 所示。

（7）打开防火墙的应用程序规则窗口，设置安全规则，如图 10-18 所示。

（8）自定义防火墙 IP 规则，如图 10-19 所示。



图 10-17　网络连接请求设置



图 10-18　应用程序规则设置



图 10-19　防火墙 IP 规则设置

(9) 修改防火墙 IP 规则,如图 10-20 所示。



图 10-20 修改 IP 规则

对主机中每一个发送和传输的数据包进行控制;向局域网内的计算机发出 ping 命令,观察能否收到应答;修改 IP 规则配置,将“允许自己用 ping 命令探测其他机器”改为禁止并保存配置,再次向局域网内同一台计算机发出 ping 命令,观察能否收到应答。

(10) 自定义防火墙安全级别,如图 10-21 所示。

(11) 观察防火墙日志,了解记录的格式和含义,如图 10-22 所示。

(12) 防火墙设置结束,如图 10-23 所示。



图 10-21　自定义防火墙安全级别



图 10-22　防火墙日志



图 10-23　设置结束

10.4　IP/MAC 地址扫描工具

10.4.1　功能简介

在网络中，计算机之间相互通信必须借助于地址。每块网络接口卡均烧录了一个全球唯一的物理地址，称为 MAC 地址，通过 MAC 地址可以对计算机进行远程管理，如远程启动等。而计算机之间的通信是通过 IP 地址进行的，IP 地址就如同人的身份证号，标识着网络中的每一台计算机，每台计算机至少要分配有一个 IP 地址。如果 IP 地址设置

错误，则计算机之间将不能正常通信。下面介绍 IP 地址和 MAC 地址工具，这些工具可以帮助管理员更好地管理网络。

10.4.2 超级扫描工具 SuperScan

SuperScan 是一种功能强大的端口扫描工具，其主要功能特性如下：

(1) 通过 ping 来检验 IP 是否在线。

(2) IP 和域名相互转换。

(3) 检验目标计算机提供的服务类别。

(4) 检验一定范围内目标计算机是否在线及端口情况。

(5) 自定义要检验的端口，并可以保存为端口列表文件。

(6) 软件自带一个木马端口列表，通过这个列表可以检测目标计算机是否有木马。用户也可以自己定义修改这个木马端口列表。

下面简要介绍 SuperScan 的基本使用方法。

(1) SuperScan 4.0 扫描工具的界面如图 10-24 所示，首先添加主机 IP。

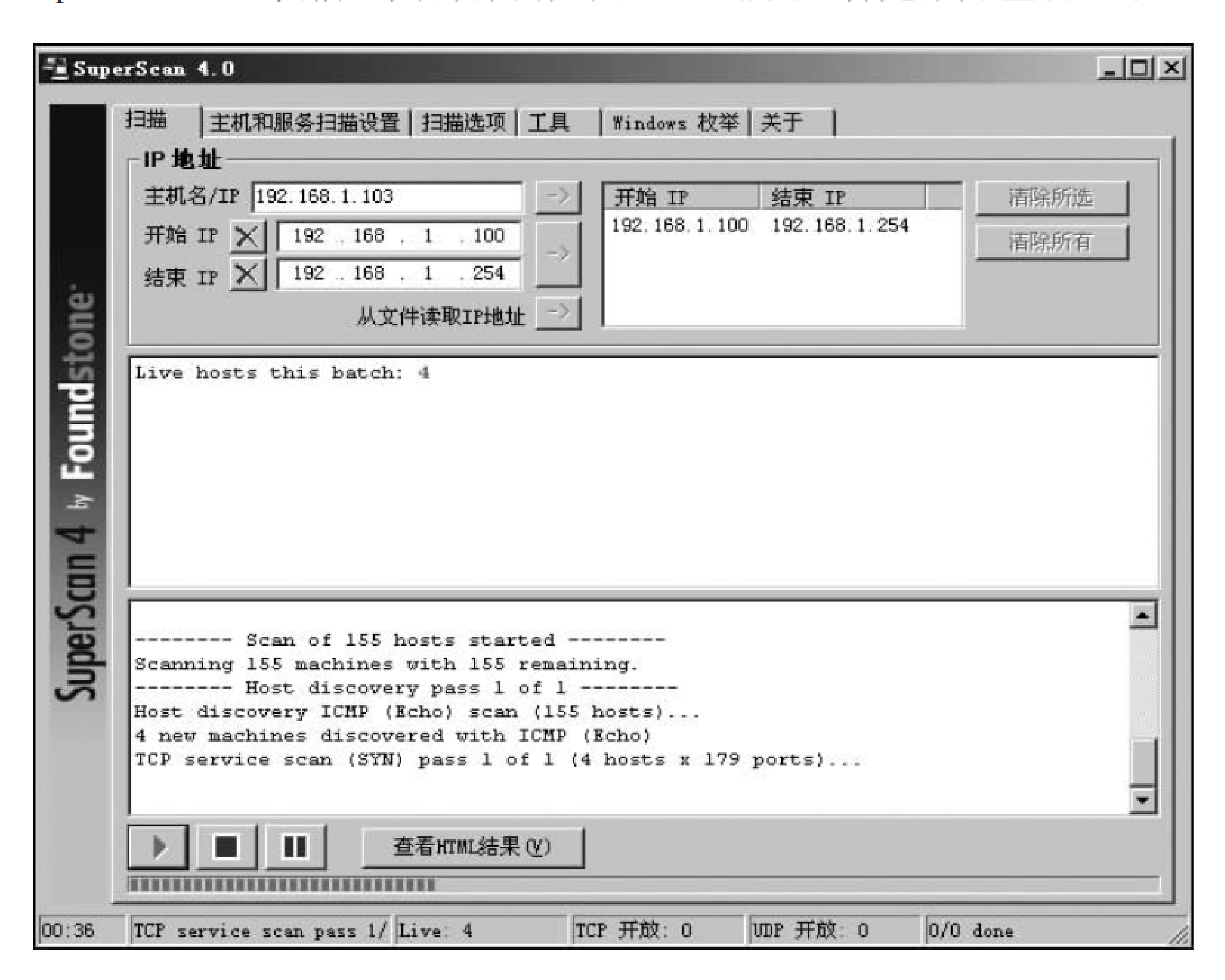


图 10-24 SuperScan 4.0 主界面

(2) 选择“主机和服务扫描设置”选项卡，分别设置要扫描的 TCP 端口及 UDP 端口列表，如图 10-25 所示。

(3) 选择“Windows 枚举”选项卡，检测目标主机操作系统中的 NetBIOS 协议、MAC 地址、用户/组以及共享等信息，如图 10-26 所示。

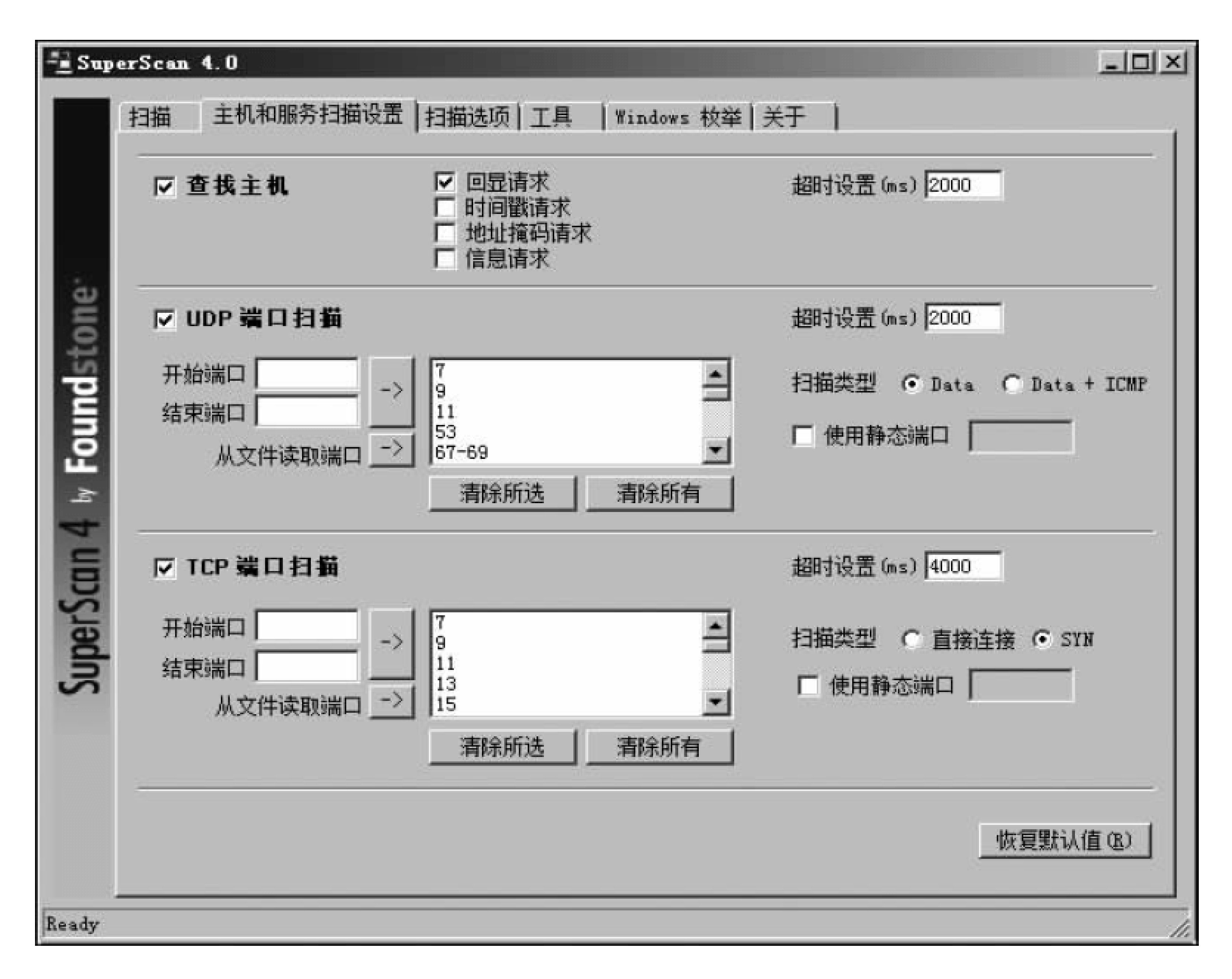


图 10-25　设置扫描端口

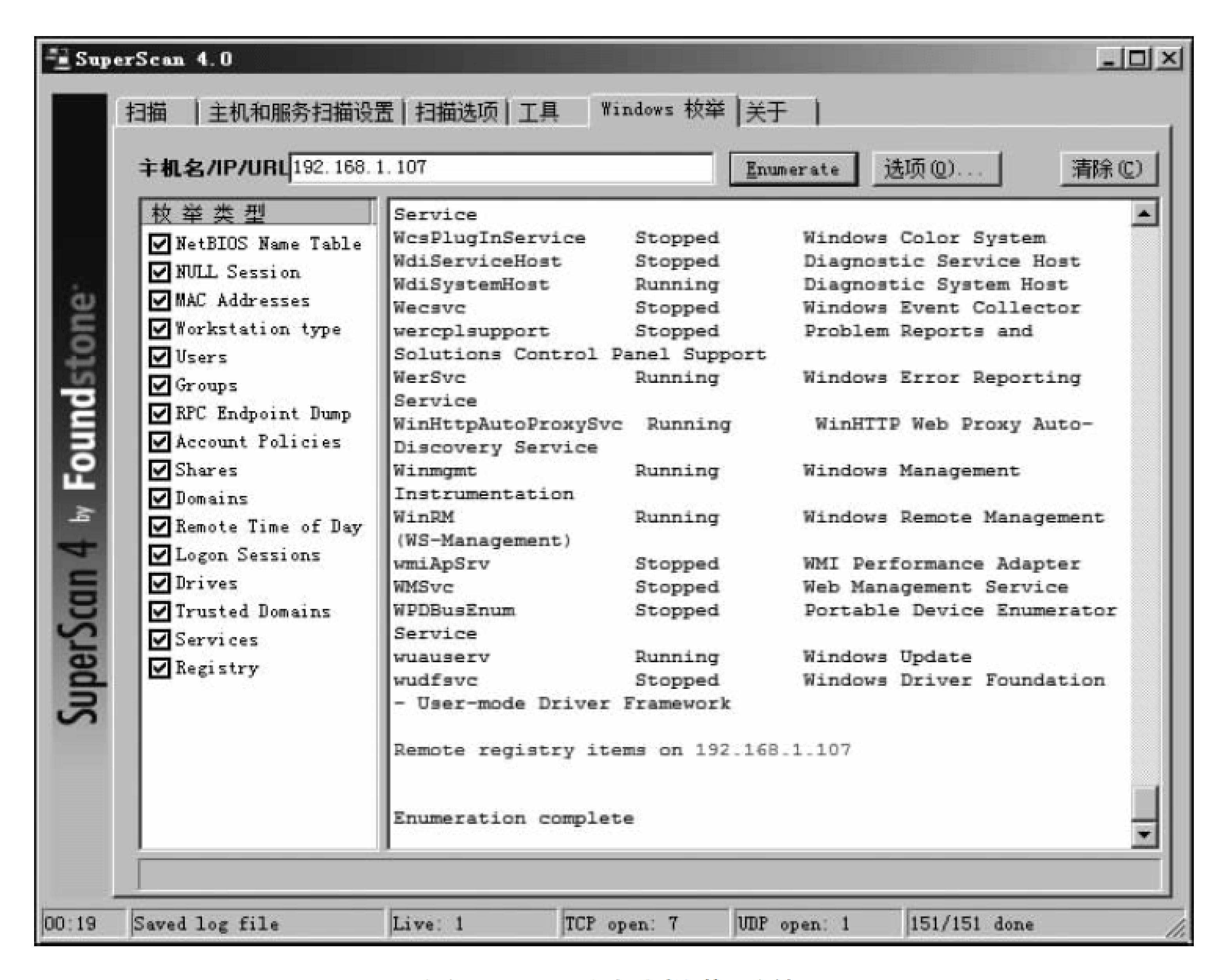


图 10-26　测试操作系统

(4) 选择“工具”选项卡，可以选取检测目标工具，如图 10-27 所示。

(5) 选择“扫描”选项卡，完成目标扫描，结果如图 10-28 所示。



图 10-27 选取检测工具

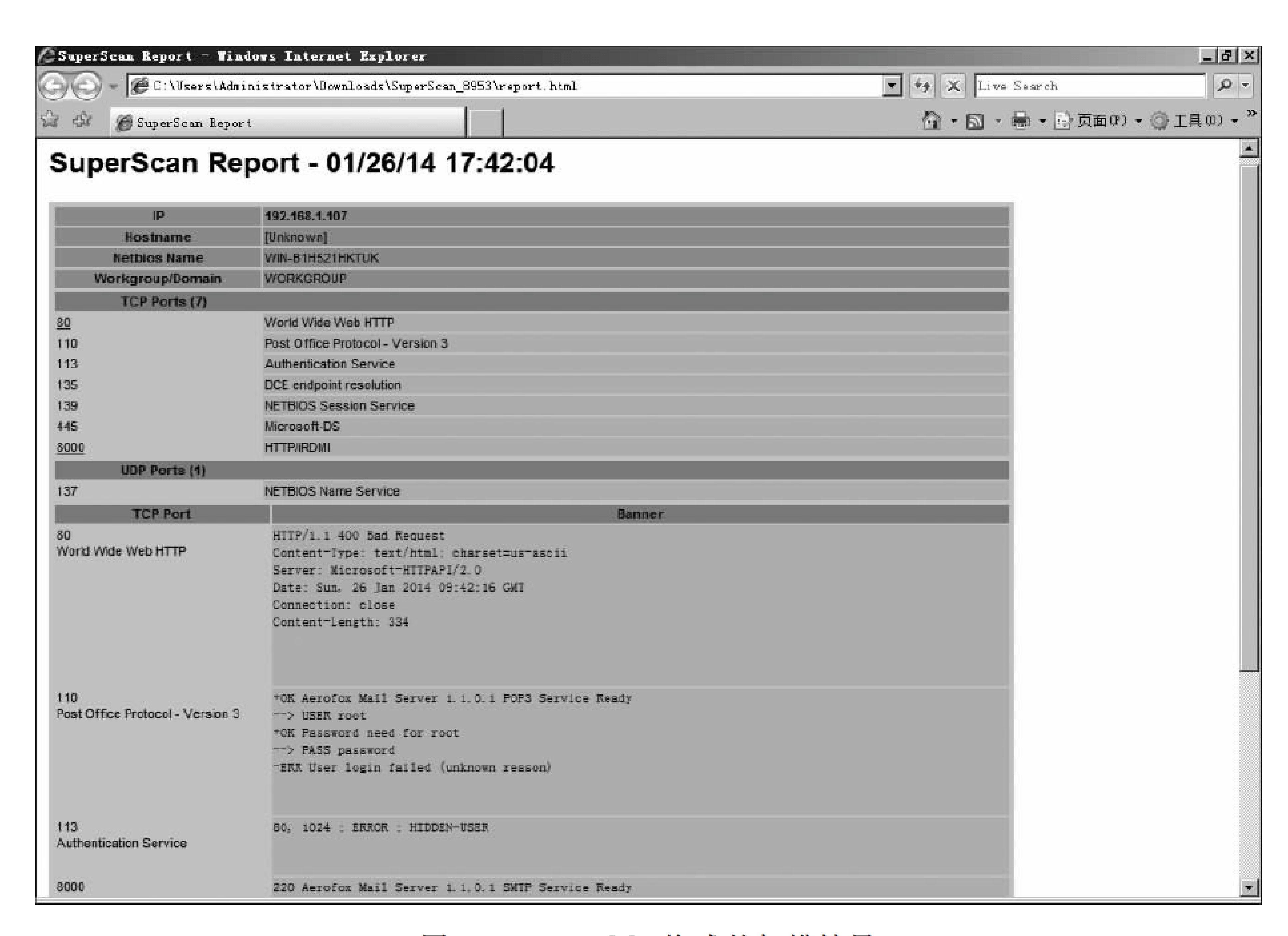


图 10-28 HTML 格式的扫描结果

10.5 IP 链路测试工具

10.5.1 功能简介

在搭建网络时，首先要保证网络链路的连通性完好，才能保证各计算机和设备之间的良好通信。因此，在网络搭建过程中，需要及时测试网络链路是否连通。网络链路分为物理链路和 IP 链路，前者主要指光纤、双绞线等介质是否物理连通，后者则是指计算机与计算机或其他设备的逻辑链接。

10.5.2 网络侦测工具 Essential NetTools

Essential NetTools(ENT)是一个网络扫描与安全管理的工具套装。其中的 NBScan 是一个监视 NetBIOS 协议扫描器，它可以侦查网内所有计算机的共享资源；NetAudit 是一个 NetBIOS 协议审核工具，为计算机网络资源共享提供安全帮助。并监视所有共享的资源。

（1）Essential NetTools 的主界面如图 10-29 所示。

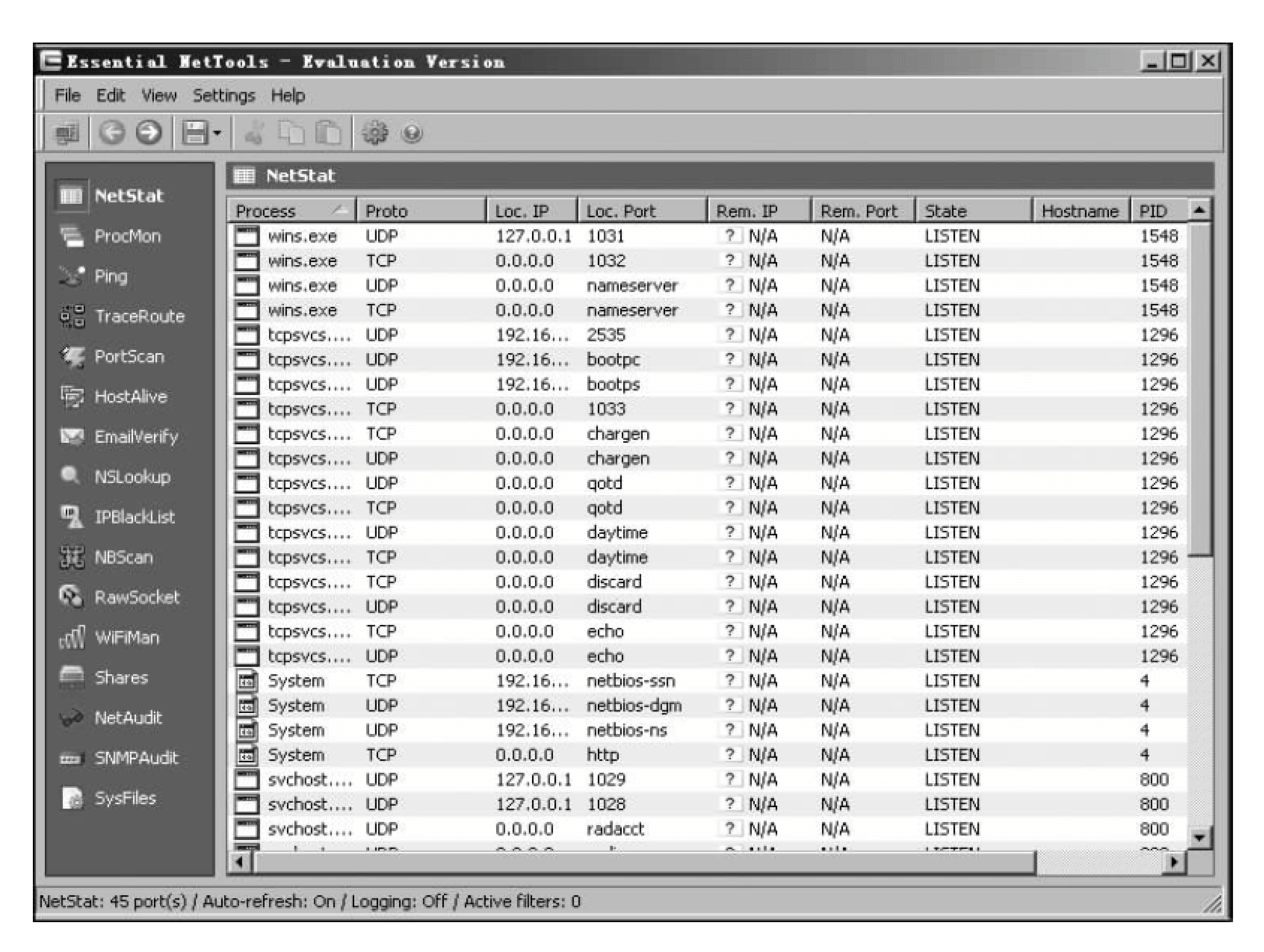


图 10-29 Essential NetTools 主界面

（2）网络系统综合侦测窗体如图 10-30 所示。

（3）主机软件运行情况侦测窗体如图 10-31 所示。

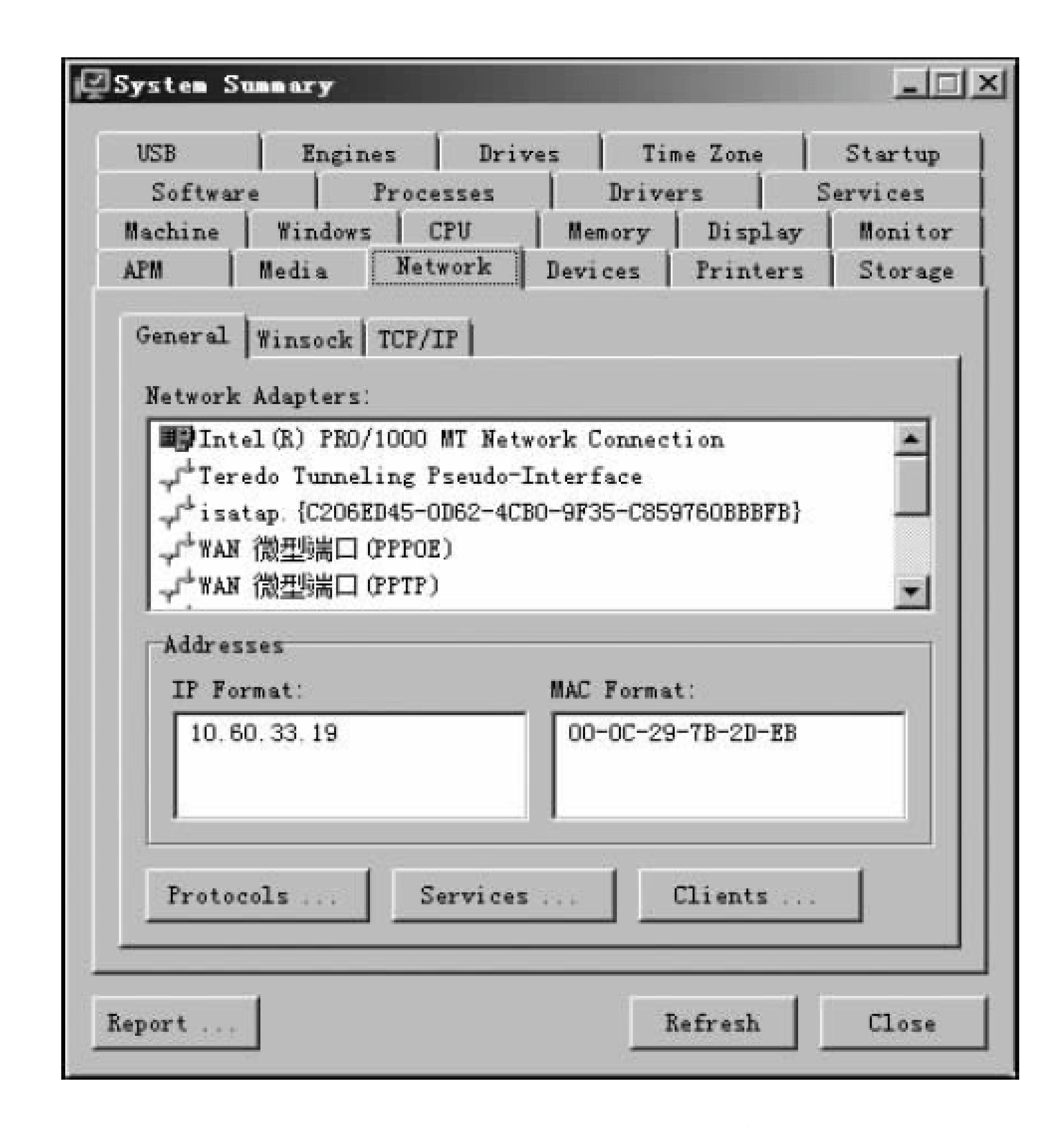


图 10-30　综合侦测窗体

图 10-31　主机软件侦测窗体

（4）主机服务项侦测窗体如图 10-32 所示。

（5）Essential NetTools 工具侦测选项设置如图 10-33 所示。

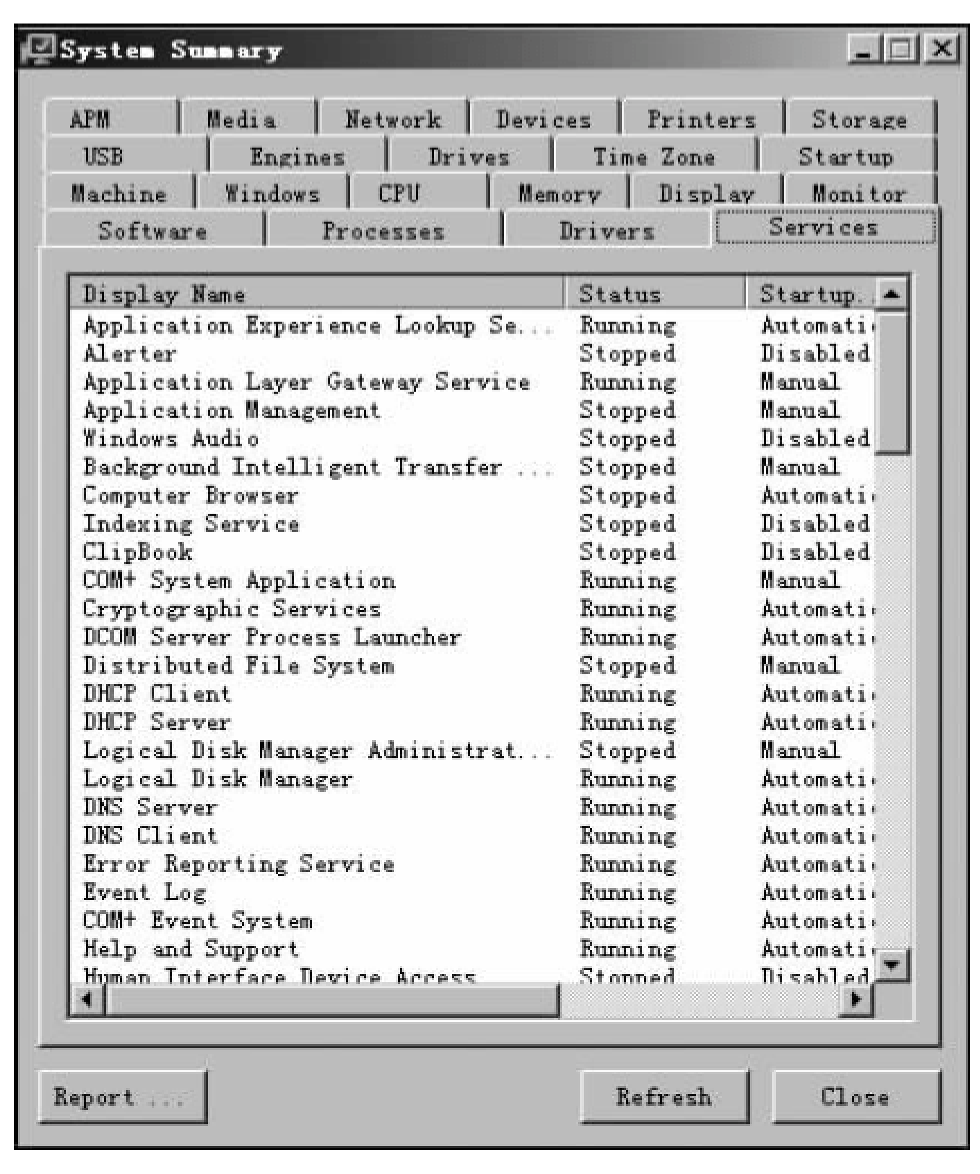


图 10-32　主机服务侦测窗体

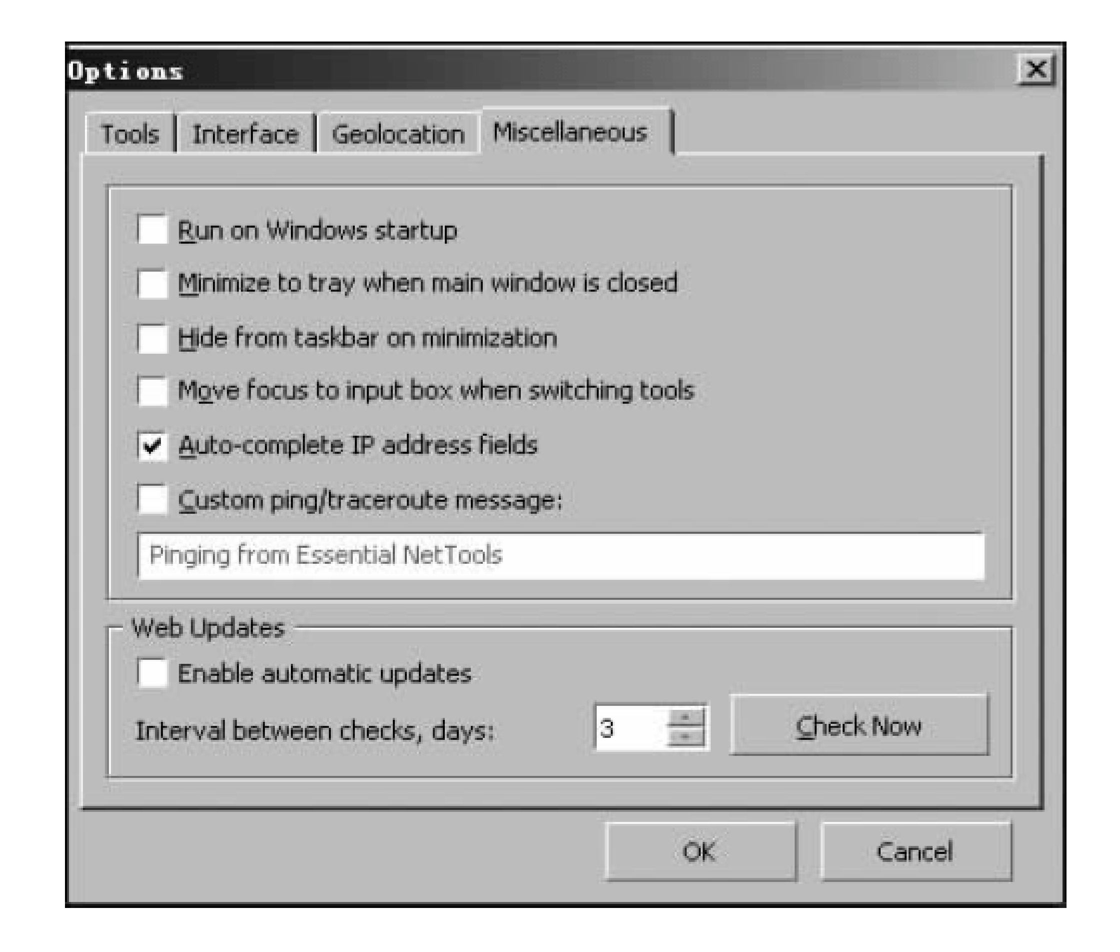


图 10-33　选项设置

（6）主机运行状况侦测窗口如图 10-34 所示。

网络侦测工具 Essential NetTools 功能强大，实用性强，对其感兴趣的读者可以查阅详细的资料。

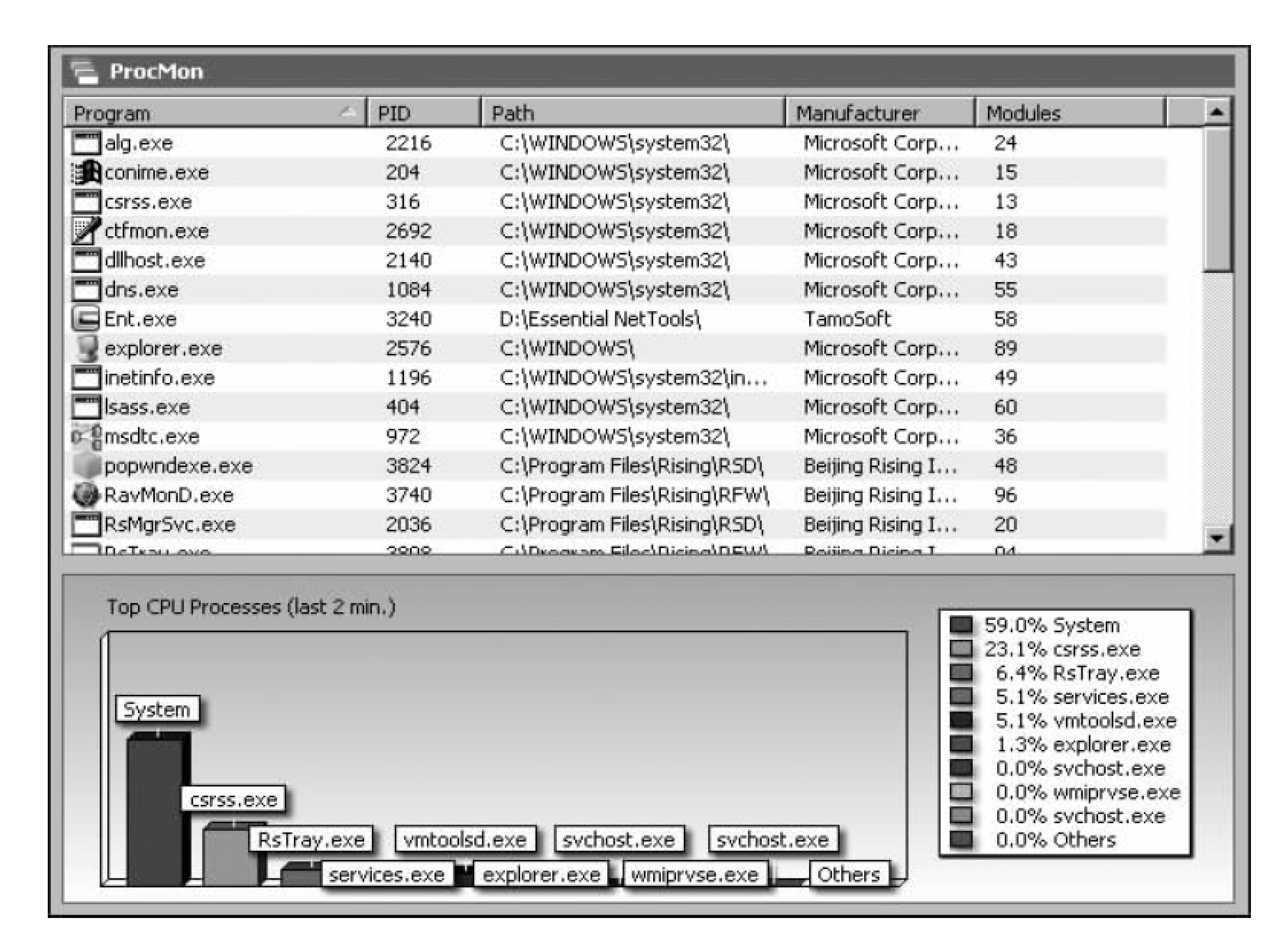


图 10-34　主机运行状况侦测

10.6　网络查看与搜索工具

10.6.1　功能简介

通常情况下，在网络中存在着很多计算机和共享资源，以及大量的 IP 地址和开放的端口等信息。为了能够充分了解并管理这些信息，管理员需要借助相关的网络查看和搜索工具来实现这一目的。

10.6.2　超级网管 SuperLANadmin

SuperLANadmin 具有强大的扫描能力，能够扫描网络上的计算机和工作组的各种有用信息，包括计算机名、工作组名、IP 地址、MAC 地址和共享文件等。它还可以实现远程关机、远程重启、发送消息、搜索共享、网络流量检测、数据包的检测、端口扫描、活动端口查看和端口进程查看。

下面简要介绍 SuperLANadmin 的基本使用方法。

（1）SuperLANadmin 的主界面如图 10-35 所示，主要功能包括网络扫描、网络管理和网络监控等。

（2）“网络扫描”功能中的“信使服务”即发送消息，如图 10-36 所示。

（3）网络扫描功能中的“共享查看”如图 10-37 所示。



图 10-35 主界面



图 10-36 信使服务



图 10-37 共享查找

该功能可以搜索局域网内的所有共享文件，当扫描到共享文件夹后，可以在指定的文件夹内按文件类型共享文件。

在扫描到的计算机列表中选中要共享资源的计算机，选择主界面左侧控制列表的“搜索共享”选项。核对选定的计算机名，选择“扫描共享”。还可以指定按文件类型扫描。

（4）网络管理功能中的“上网权限设置”如图 10-38 所示。

（5）网络管理功能中的“端口扫描”如图 10-39 所示。

端口是计算机的通信通道，也是入侵通道，对目标计算机进行端口扫描能得到许多有用信

图 10-38 上网权限设置

息。根据需要输入本地或者远程计算机的 IP 地址，扫描常用的端口或者端口的范围。

（6）网络管理功能中的“域名解析”如图 10-40 所示。



图 10-39　端口扫描



图 10-40　域名解析

10.7　流量监控与分析工具

10.7.1　功能简介

无论网络性能有多么强大，都有可能因为某些用户滥用网络资源而导致网络性能下降，甚至造成网络瘫痪。因此，管理员应时刻关注网络中的流量情况，保证用户可以充分、合理地利用网络资源，杜绝用户对网络资源的恶意占用。

10.7.2　流量分析器 CommView

CommView 是进行网络流量统计分析的一个利器，可以捕获局域网中所有计算机和外部网络间传输的数据。管理员通过分析这些数据可以清楚地了解到网络的运行状况。

下面简要介绍 CommView 的基本使用方法。

（1）单击工具栏中的开始捕获按钮，CommView 便开始捕获网络内传输的数据，如图 10-41 所示，捕获的数据包括各个网络连接的各种信息、本地地址（Local IP）、远程 IP 地址（Remote IP ）、传入数据量（In）、传出数据量（Out）、数据传输方向（Direction）和传输字节数（Bytes）等。

（2）单击工具栏中的停止捕获按钮即可停止捕获。这里可以清楚地看到本地计算机正在与外部网络的哪些地址进行通信，有哪些可疑端口正在使用。选择 VoIP 选项卡查看协议的详细信息，如图 10-42 所示，该选项卡共分为 3 个窗格，最上面的窗格中显示了协议、地址、端口以及时间等信息，中间窗格以十六进制代码显示信息，最下面的窗格显示了所有传输的信息。

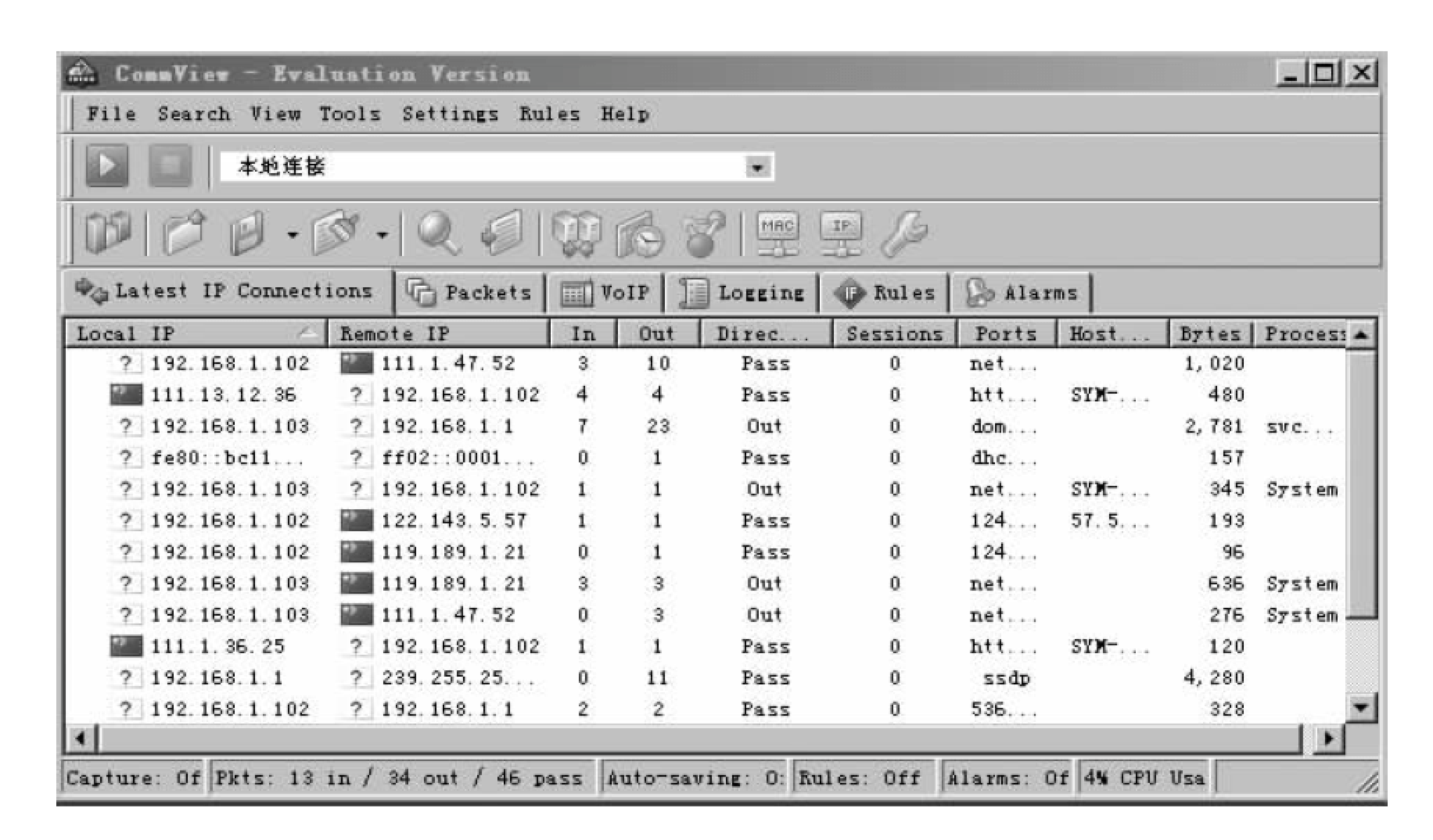


图 10-41　主机流量分析

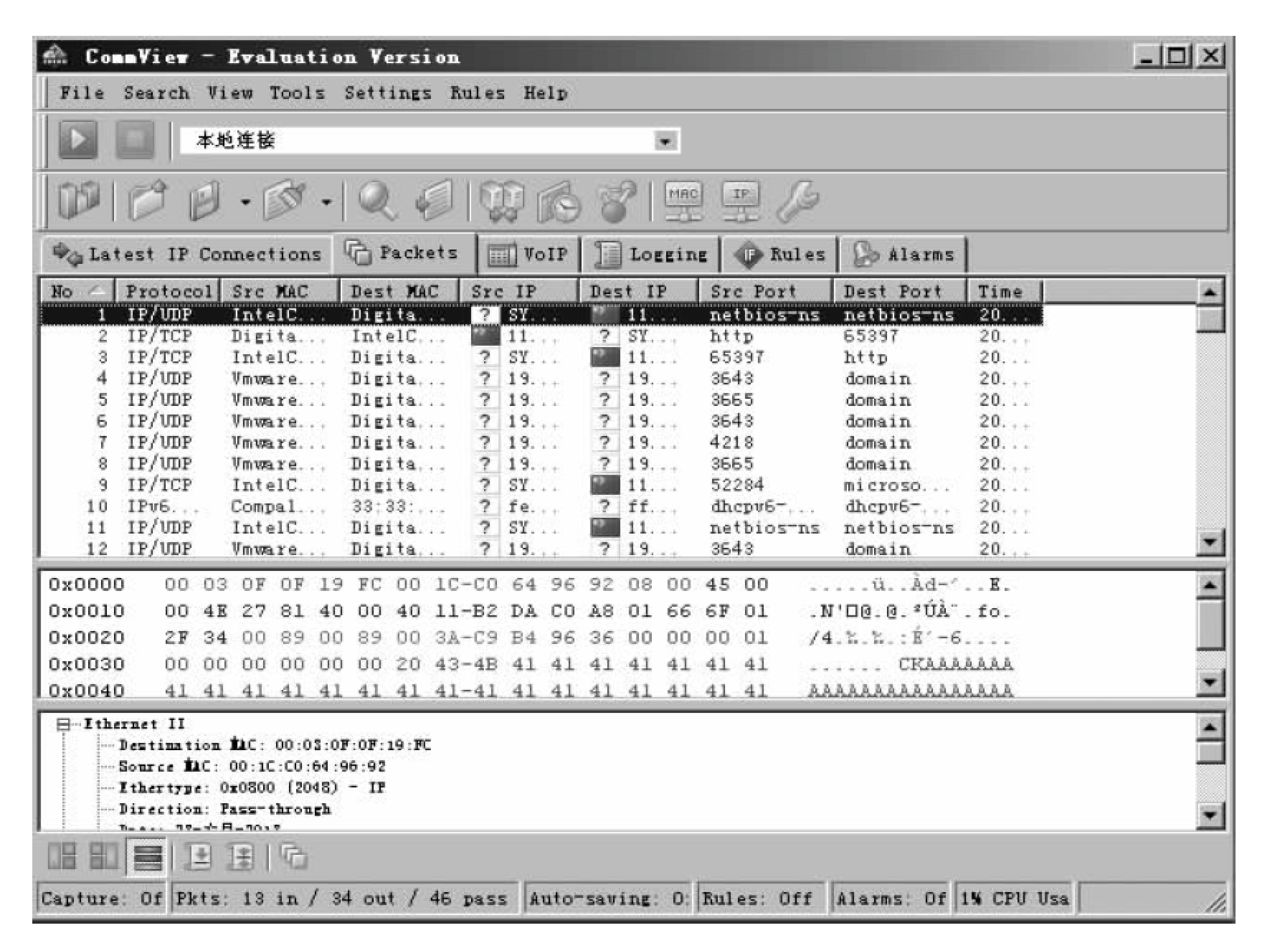


图 10-42　协议端口信息

（3）捕获设置如图 10-43 所示。

（4）捕获设置中的常规(General)选项设置如图 10-44 所示。

（5）流量统计分析如图 10-45 所示。

图 10-43　捕获设置

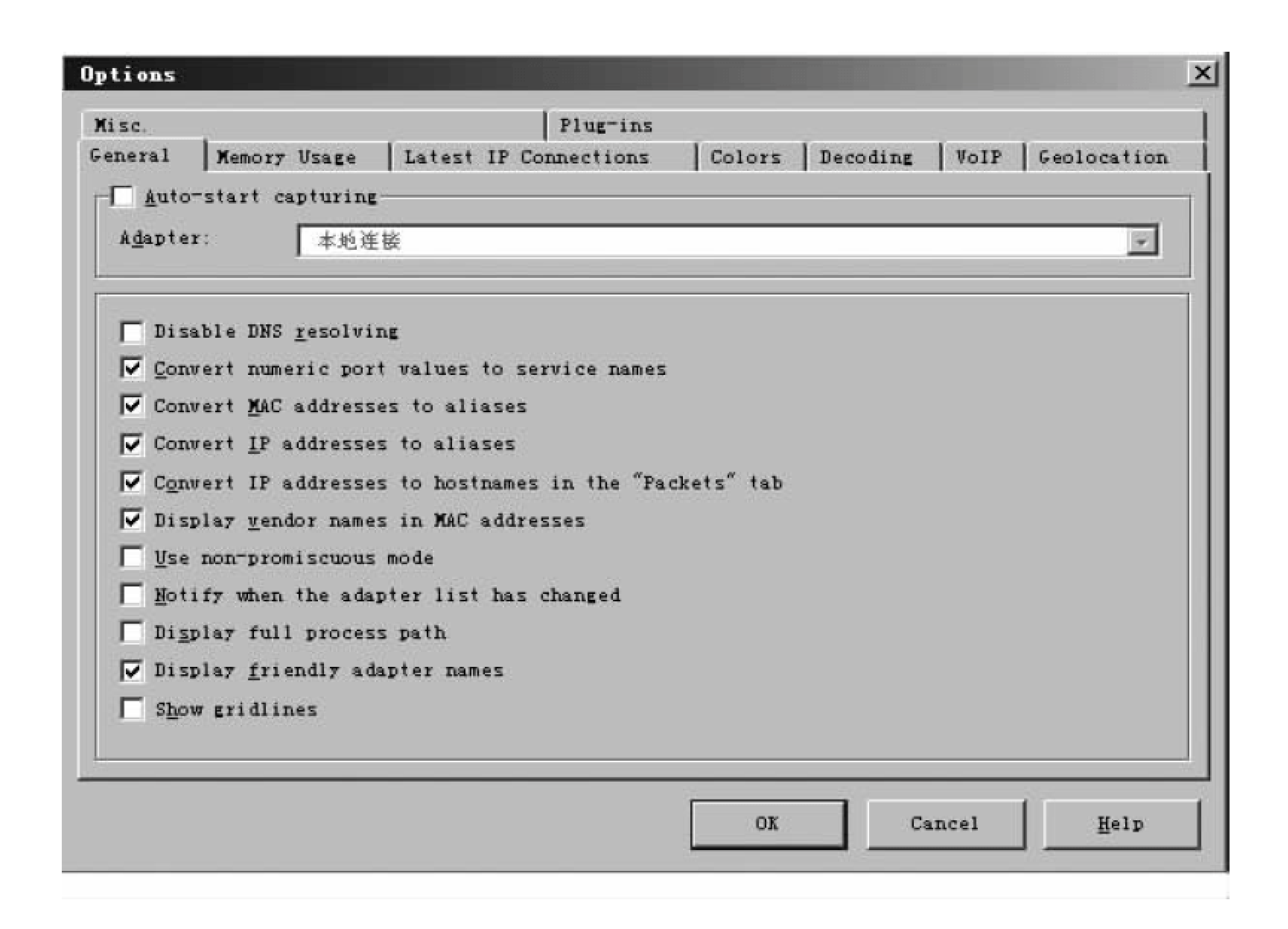


图 10-44　捕获常规设置

(6) 本地连接分析如图 10-46 所示。

(7) 指定主机按协议、MAC 地址以及 IP 地址组合规则筛选捕获，如图 10-47 所示。

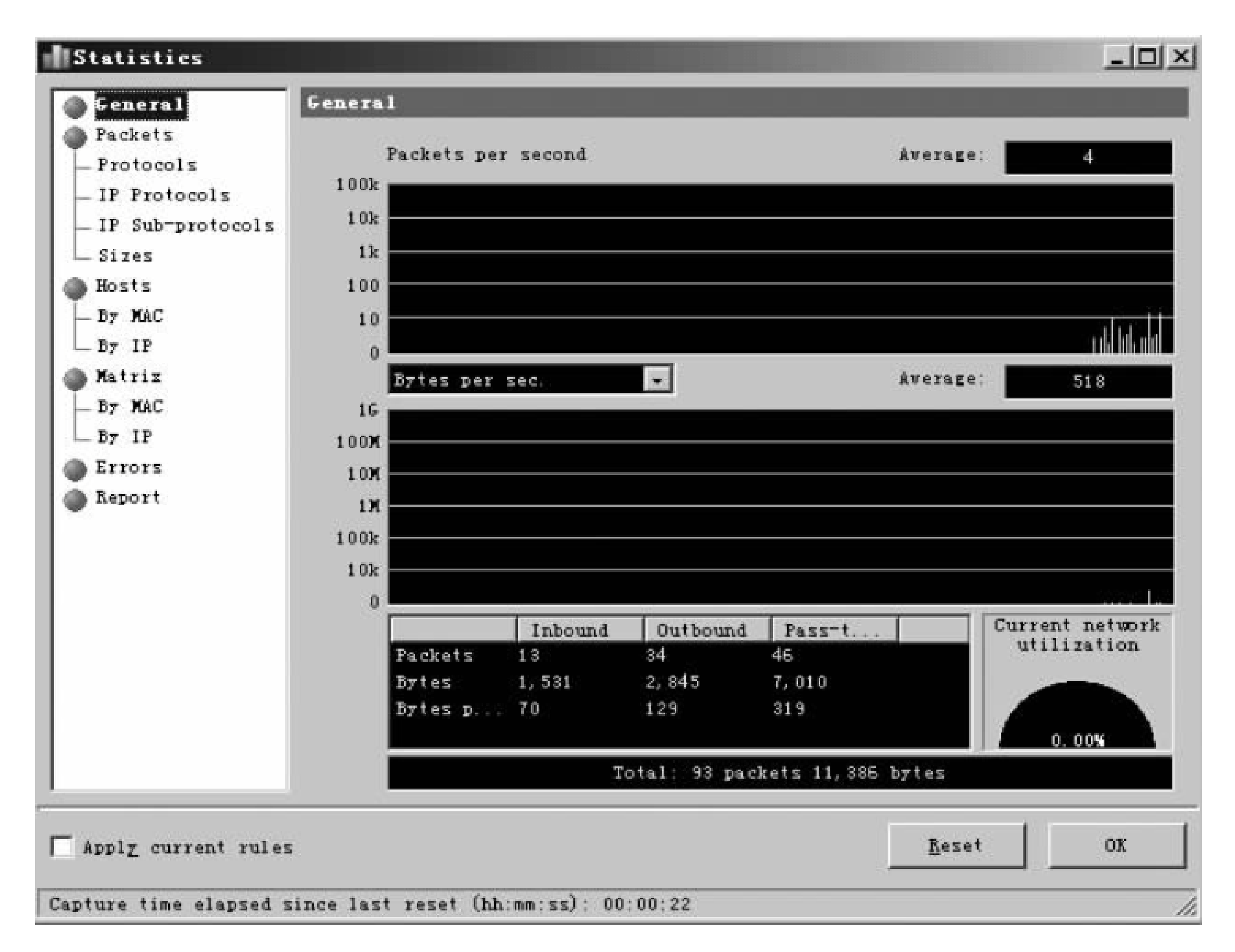


图 10-45　流量分析

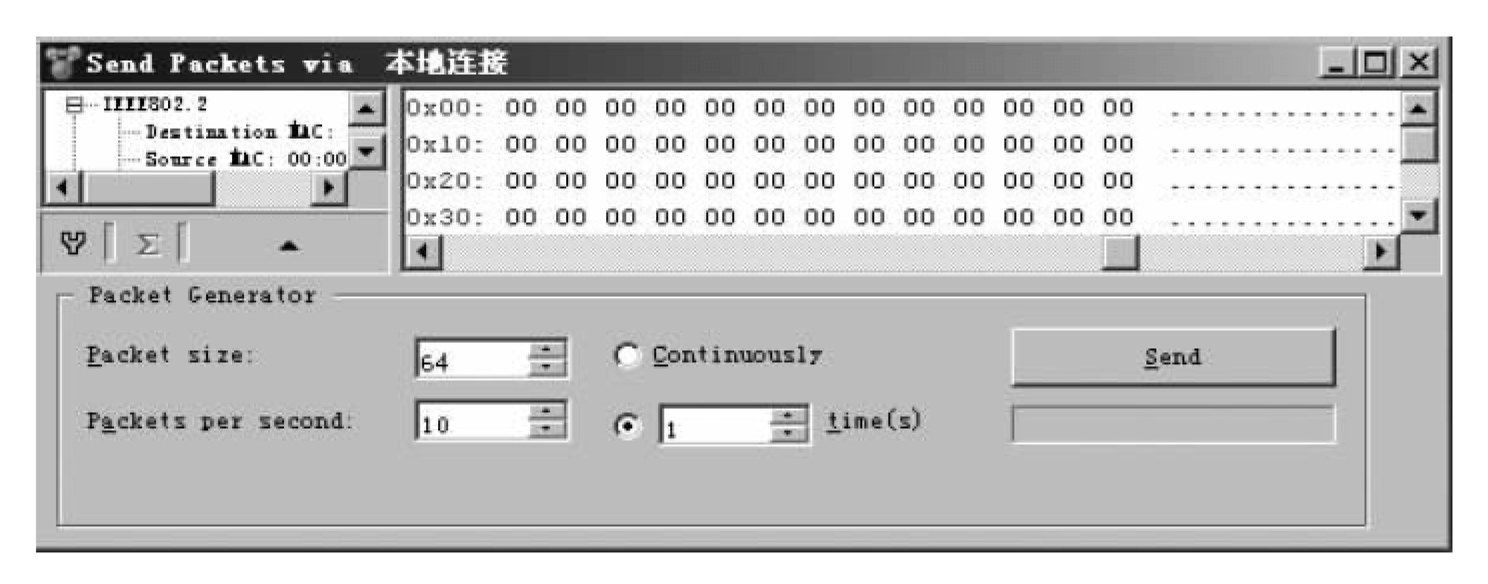


图 10-46　本地连接分析

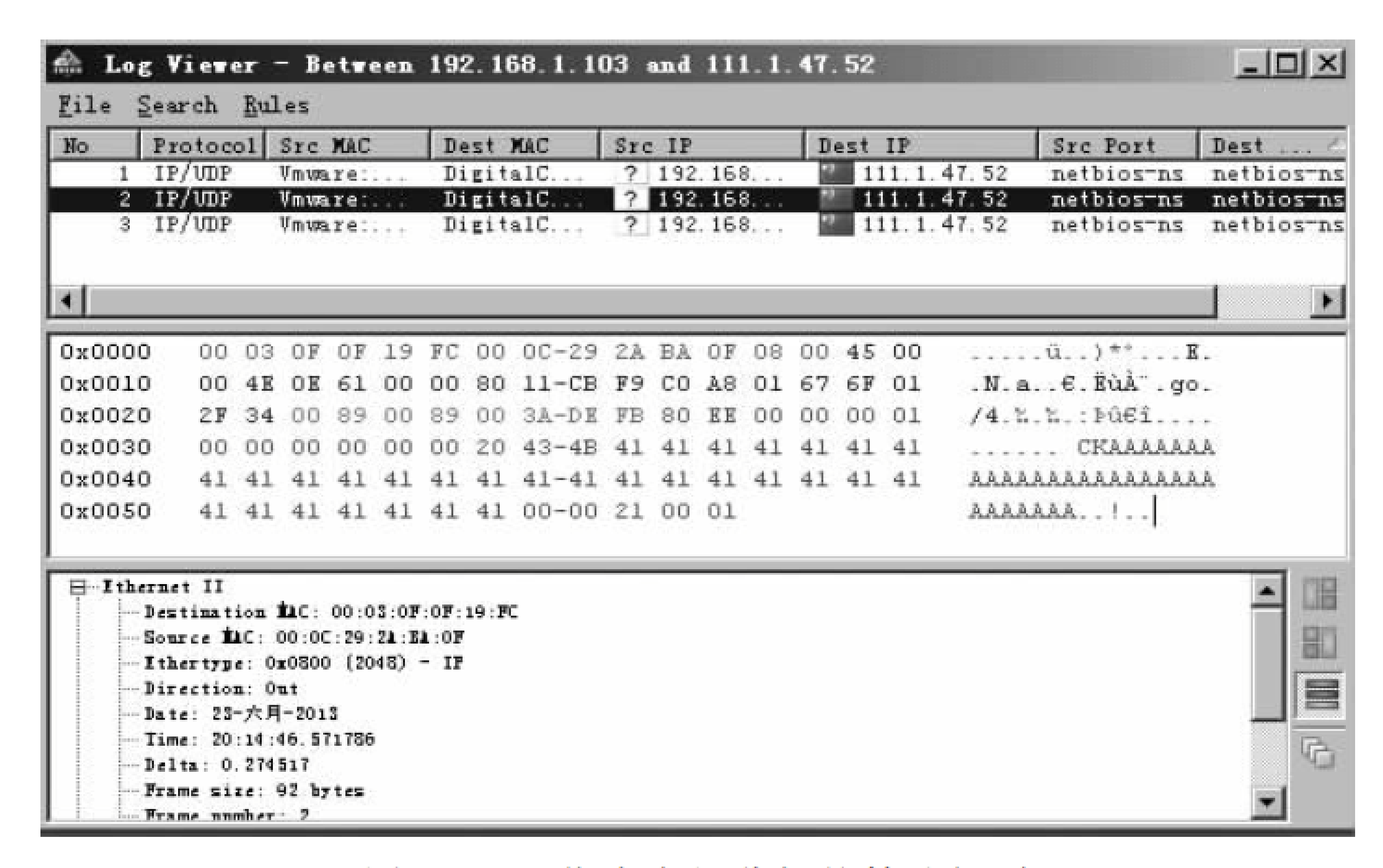


图 10-47　指定主机分析的筛选规则

10.8 服务器监控工具

10.8.1 功能简介

对网络服务器进行管理和监控，可以提前发现故障，以尽可能将损失减少到最低。在网络中，使用得最多的服务有活动目录服务、DHCP 服务、DNS 服务、文件服务、Web 服务、FTP 服务、E-mail 服务和视频点播服务等。在多数情况下，服务器会部署在网络中的不同位置，所以对服务器的监控和管理是一件比较困难的事。借助服务器管理和监控工具，管理员可以轻松地实现服务器的管理和监控。

10.8.2 监视服务器工具 Simple Server Monitor

Simple Server Monitor 是一款非常实用的监控服务工具，功能齐全，直观方便，包含精确到 60 秒内的运行时间监控以及性能图表。

下面简要介绍 Simple Server Monitor 的基本使用方法。

(1) Simple Server Monitor 的主界面如图 10-48 所示。

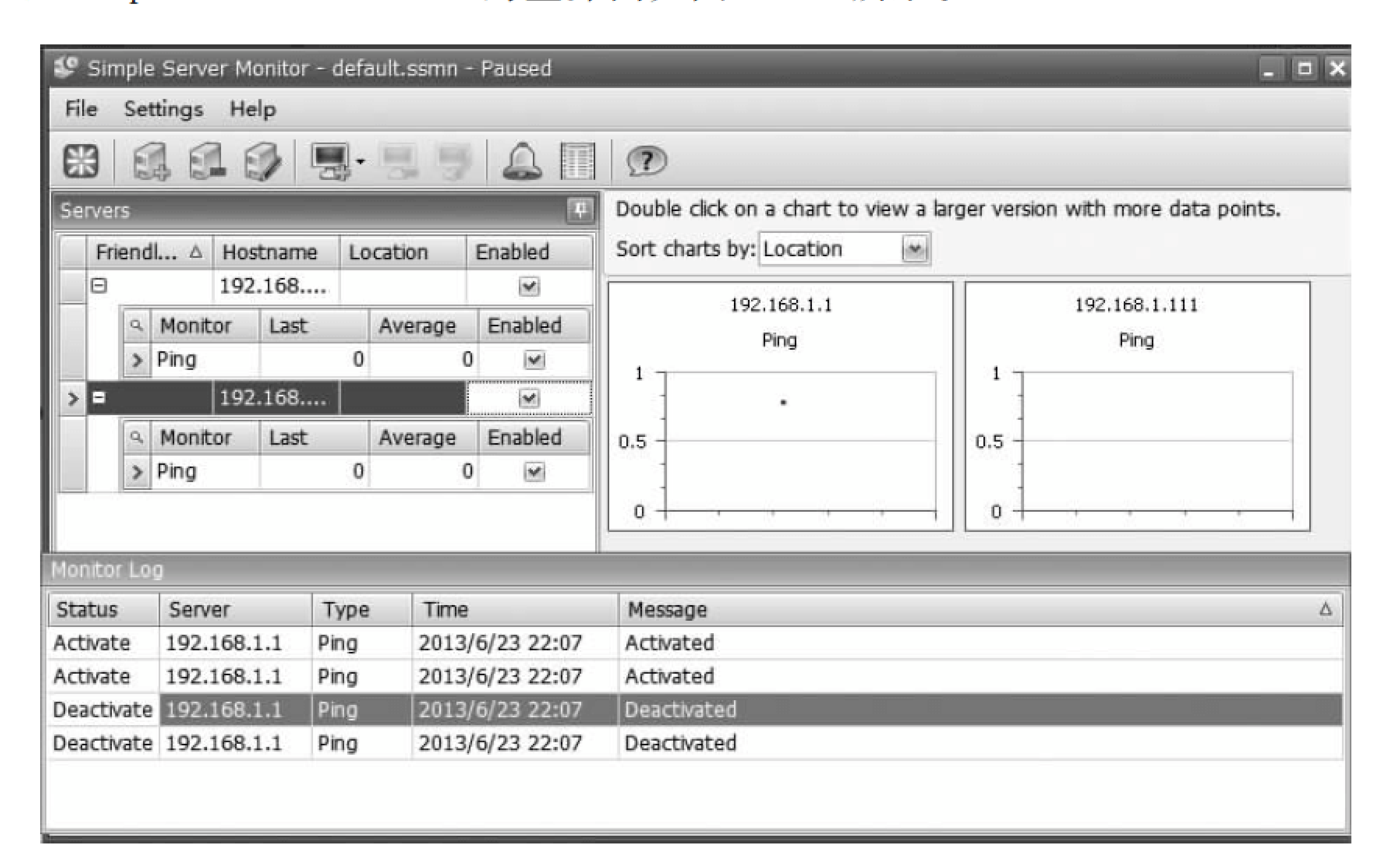


图 10-48 Simple Server Monitor 的主界面

(2) 设置跟踪主机类别，如图 10-49 所示。

(3) 选择跟踪主机服务协议，如图 10-50 所示。

(4) 添加跟踪服务器，输入其主机名(Hostname)，观察机 Location 等信息，如图 10-51 所示。

(5) 服务监视反馈如图 10-52 所示。

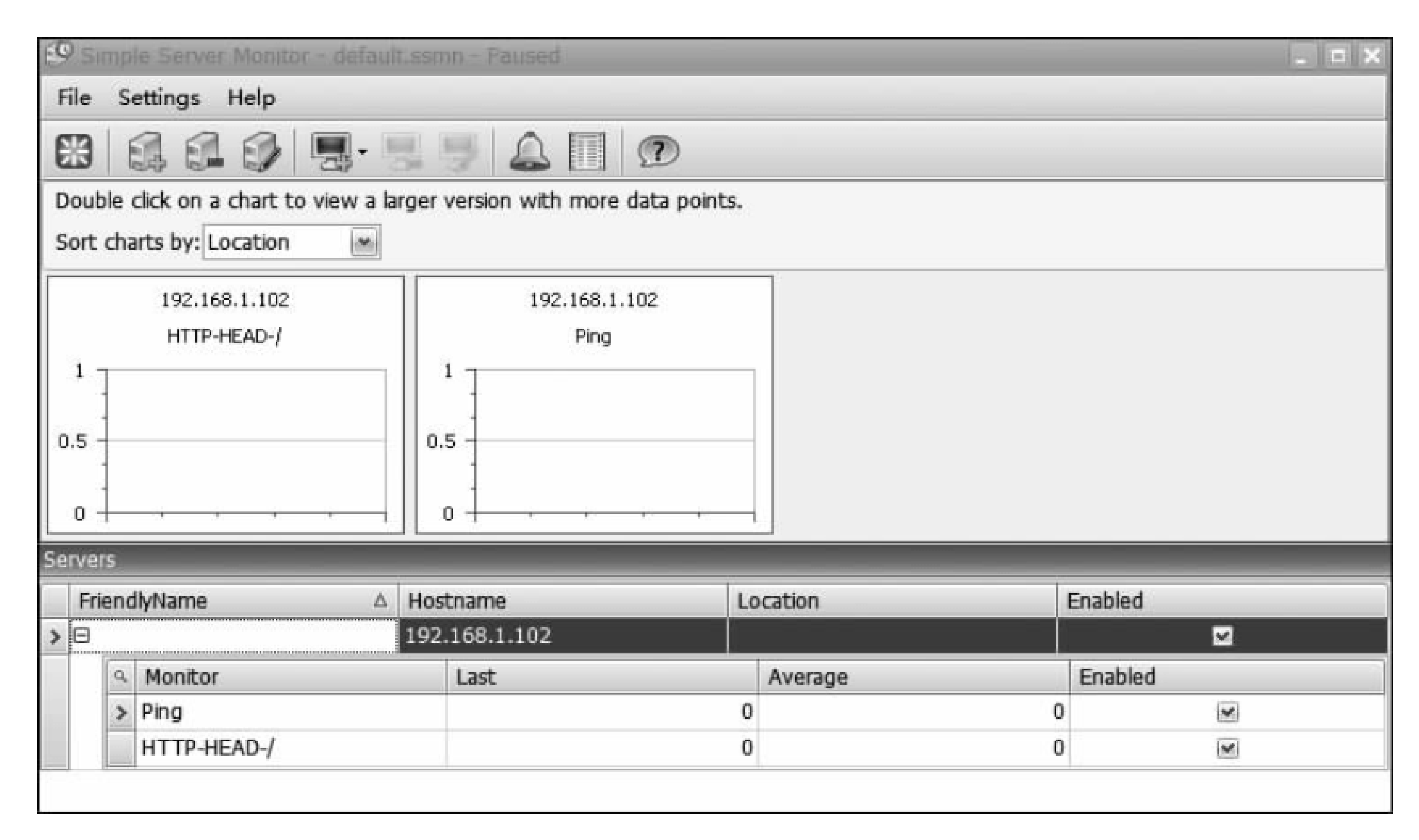


图 10-49 设置主机类别

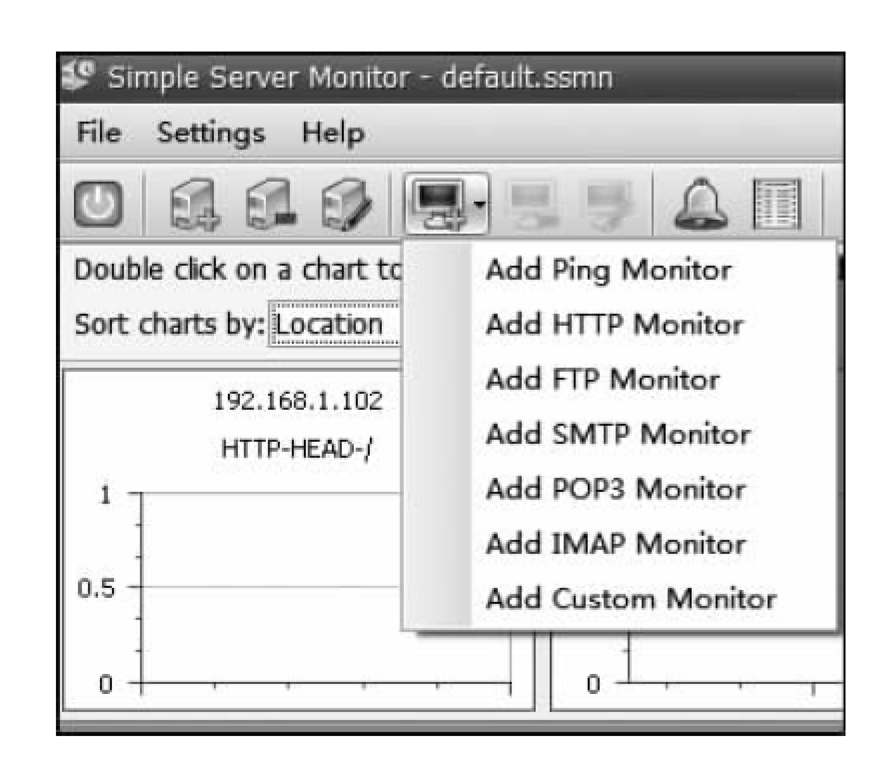


图 10-50 选择服务协议

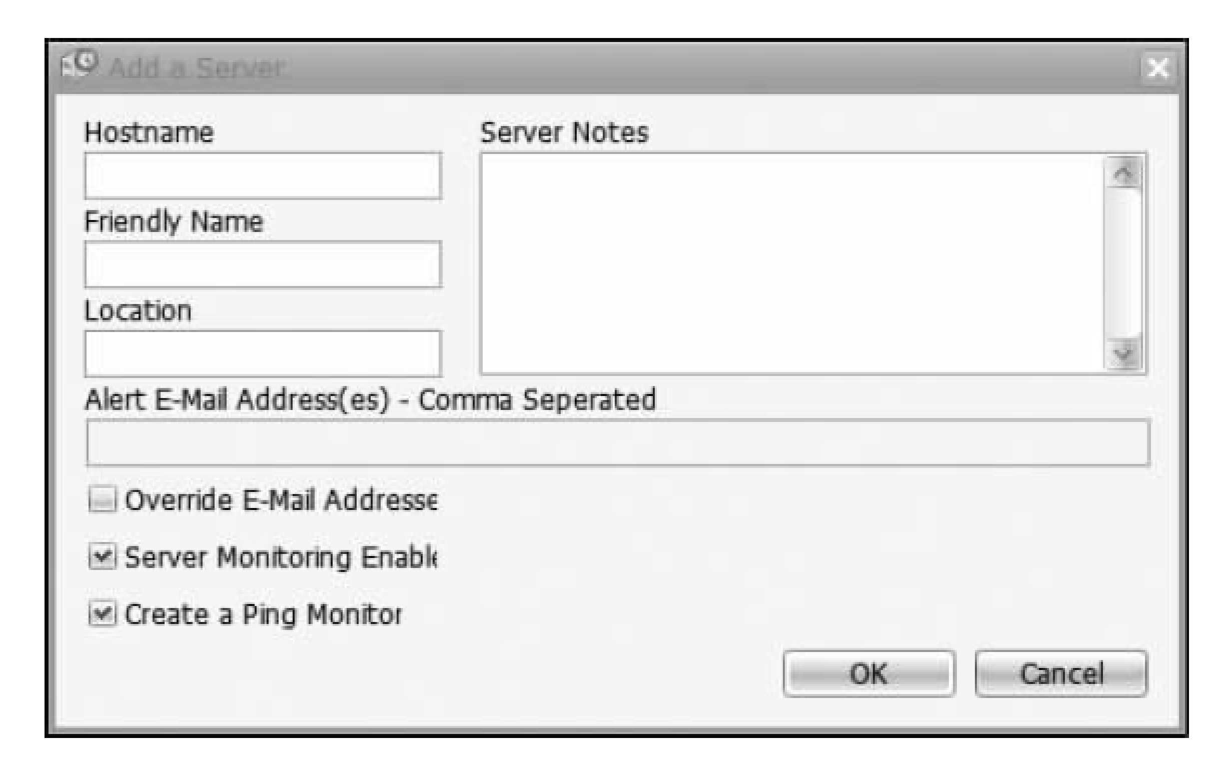


图 10-51 添加跟踪服务器



图 10-52 反馈信息

(6) 添加监视服务器,如图 10-53 所示。

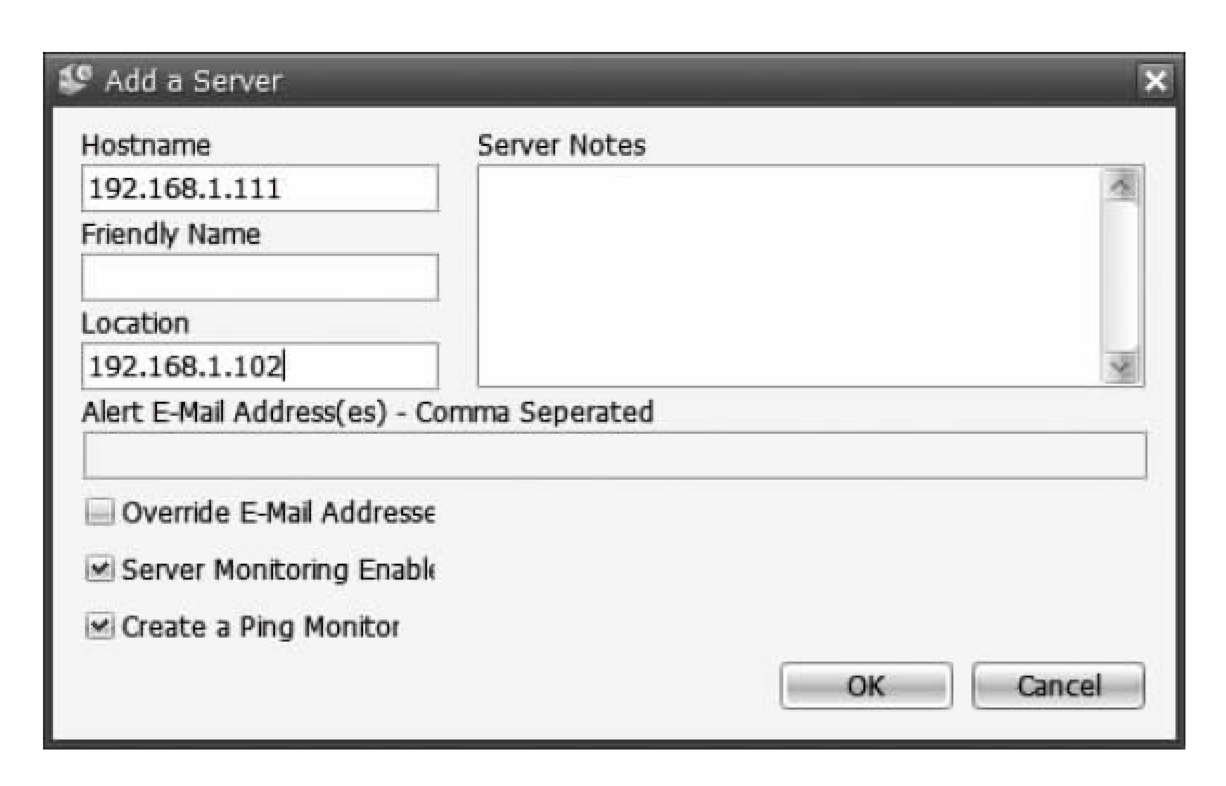


图 10-53　添加监视服务器

(7) 监视反馈信息如图 10-54 所示。

(8) 根据实际工作情况进行监视服务设置,如图 10-55 所示。

Simple Server Monitor Alert
Monitor Failed
Time: 2013/6/23 22:31
Server: 192.168.1.111
Location: 192.168.1.102
Monitor: Ping
Port: 7
Message: Timeout

图 10-54　监视反馈信息

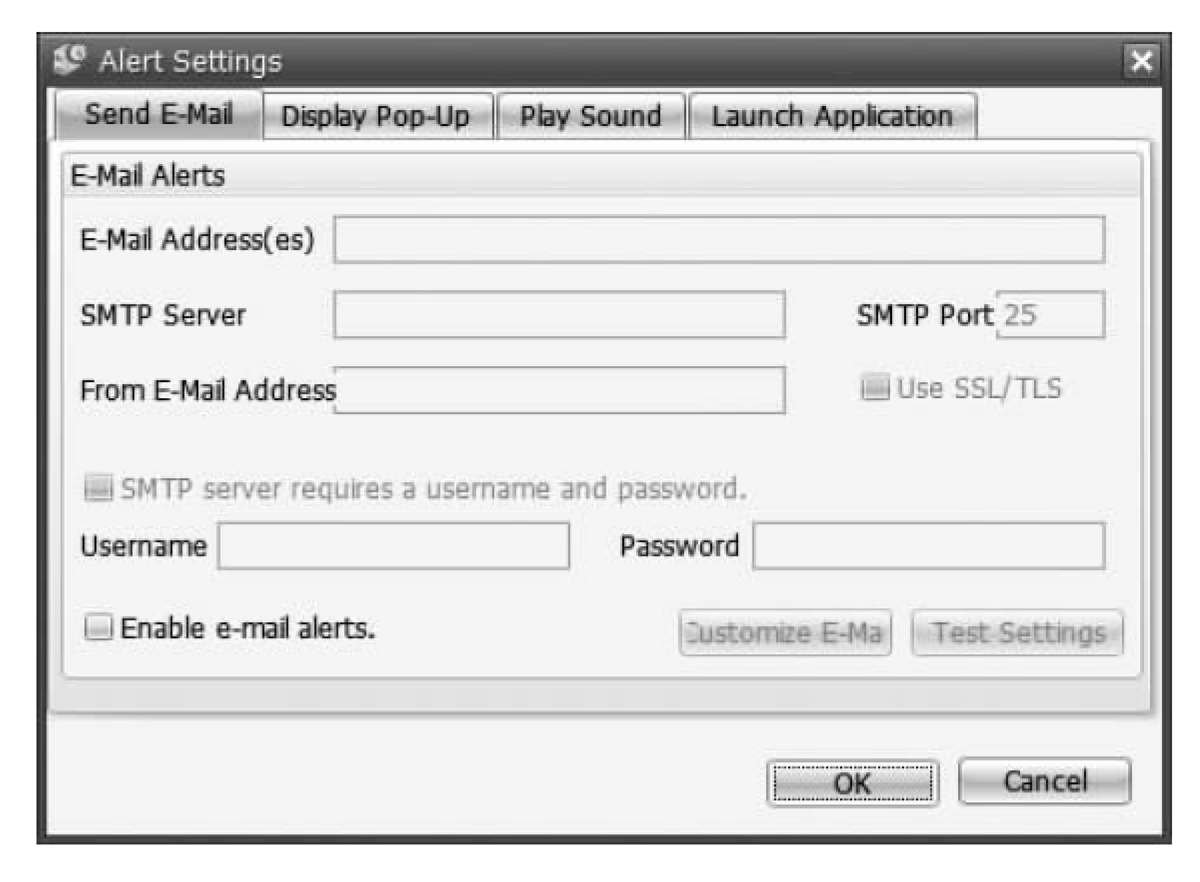


图 10-55　监视服务设置

10.9　本章小结

本章介绍了安全漏洞扫描器 X-Scan、网络数据包分析软件 Wireshark、天网个人防火墙设置、超级扫描工具 SuperScan、网络侦测工具 Essential NetTools、超级网管 SuperLANadmin、流量分析器 CommView 以及服务监控工具 Simple Server Monitor 共 8 个网管工具。

本章介绍的网络安全管理工具基本涵盖了网络扫描、网络管理、网络监测以及系统配置等网络安全管理的全过程,每个工具各有所长,在实际工作可以根据需要进行选择。

附录 A　常用端口列表

A. 1　TCP 端口

7＝回显
9＝丢弃
11＝在线用户
13＝时间服务
15＝网络状态
17＝每日引用
18＝消息发送
19＝字符发生器
20＝FTP 数据
21＝文件传输
22＝SSH 端口
23＝远程终端
25＝发送邮件
31＝Masters Paradise 木马
37＝时间
39＝资源定位协议
41＝DeepThroat 木马
42＝WINS 主机名服务
43＝WHOLS 服务
58＝DMSetup 木马
59＝个人文件服务
63＝WHOIS 端口
69＝TFTP 服务
70＝信息检索
79＝查询在线用户
80＝Web 网页
88＝Kerberos5 认证
101＝主机名
102＝ISO
107＝远程登录终端
109＝POP2 邮件
110＝POP3 邮件
111＝SUN 远程控制
113＝身份验证
117＝UUPC
119＝NNTP 新闻组
121＝JammerKillah 木马
135＝本地服务
138＝隐形大盗
139＝文件共享
143＝IMAP4 邮件
146＝FC-Infector 木马
158＝邮件服务
170＝打印服务
179＝BGP
194＝IRC 端口
213＝TCP over IPX
220＝IMAP3 邮件
389＝目录服务
406＝IMSP 端口
411＝DC＋＋
421＝TCP Wrappers
443＝安全 Web 访问
445＝SMB(交换服务器消息块)
456＝Hackers Paradise 木马
464＝Kerberos 认证
512＝远程执行或卫星通信
513＝远程登录与查询
514＝SHELL/系统日志
515＝打印服务
517＝Talk
518＝网络聊天
520＝EFS
525＝时间服务
526＝日期更新
530＝RPC
531＝RASmin 木马
532＝新闻阅读

533＝紧急广播
540＝UUCP
543＝Kerberos 登录
544＝远程 Shell
550＝Who
554＝RTSP
555＝Ini-Killer 木马
556＝远程文件系统
560＝远程监控
561＝监控
636＝安全目录服务
666＝Attack FTP 木马
749＝Kerberos 管理
750＝Kerberos V4
911＝Dark Shadow 木马
989＝FTPS
990＝FTPS
992＝Telnets
993＝IMAPS
999＝DeepThroat 木马
1001＝Silencer 木马
1010＝Doly 木马
1011＝Doly 木马
1012＝Doly 木马
1015＝Doly 木马
1024＝NetSpy 木马
1042＝Bla 木马
1045＝RASmin 木马
1080＝SOCKS 代理
1090＝Extreme 木马
1095＝Rat 木马
1097＝Rat 木马
1098＝Rat 木马
1099＝Rat 木马
1109＝Kerberos POP
1167＝私用电话
1170＝Psyber Stream Server
1214＝KAZAA 下载
1234＝Ultors/恶鹰木马
1243＝Backdoor/SubSeven 木马
1245＝VooDoo Doll 木马
1349＝BO DLL 木马
1352＝Lotus Notes
1433＝SQL Server
1492＝FTP99CMP 木马
1494＝CITRIX
1503＝NetMeeting
1512＝WINS 解析
1524＝IngresLock 后门
1600＝Shivka-Burka 木马
1630＝网易泡泡
1701＝L2TP
1720＝H323
1723＝PPTP(虚拟专用网)
1731＝NetMeeting
1755＝流媒体服务
1807＝SpySender 木马
1812＝Radius 认证
1813＝Radius 评估
1863＝MSN 聊天
1981＝ShockRave 木马
1999＝Backdoor 木马
2000＝TransScout-Remote-Explorer 木马
2001＝TransScout 木马
2002＝TransScout/恶鹰木马
2003＝TransScout 木马
2004＝TransScout 木马
2005＝TransScout 木马
2023＝Ripper 木马
2049＝NFS 服务器
2053＝KNETD
2115＝Bugs 木马
2140＝DeepThroat 木马
2401＝CVS
2535＝恶鹰木马
2565＝Striker 木马
2583＝WinCrash 木马
2773＝Backdoor/SubSeven 木马
2774＝SubSeven 木马
2801＝Phineas Phucker 木马
2869＝UPnP(通用即插即用)
3024＝WinCrash 木马
3050＝InterBase
3128＝squid 代理

3129＝Masters Paradise 木马
3150＝DeepThroat 木马
3306＝MySQL
3389＝远程桌面
3544＝MSN 语音
3545＝MSN 语音
3546＝MSN 语音
3547＝MSN 语音
3548＝MSN 语音
3549＝MSN 语音
3550＝MSN 语音
3551＝MSN 语音
3552＝MSN 语音
3553＝MSN 语音
3554＝MSN 语音
3555＝MSN 语音
3556＝MSN 语音
3557＝MSN 语音
3558＝MSN 语音
3559＝MSN 语音
3560＝MSN 语音
3561＝MSN 语音
3562＝MSN 语音
3563＝MSN 语音
3564＝MSN 语音
3565＝MSN 语音
3566＝MSN 语音
3567＝MSN 语音
3568＝MSN 语音
3569＝MSN 语音
3570＝MSN 语音
3571＝MSN 语音
3572＝MSN 语音
3573＝MSN 语音
3574＝MSN 语音
3575＝MSN 语音
3576＝MSN 语音
3577＝MSN 语音
3578＝MSN 语音
3579＝MSN 语音
3700＝Portal of Doom 木马
4080＝WebAdmin
4081＝WebAdmin＋SSL
4092＝WinCrash 木马
4267＝SubSeven 木马
4443＝AOL MSN
4567＝File Nail 木马
4590＝ICQ 木马
4661＝电驴下载
4662＝电驴下载
4663＝电驴下载
4664＝电驴下载
4665＝电驴下载
4666＝电驴下载
4899＝Radmin 木马
5000＝Sokets-de 木马
5000＝UPnP(通用即插即用)
5001＝Back Door Setup 木马
5060＝SIP
5168＝高波蠕虫
5190＝AOL MSN
5321＝Firehotcker 木马
5333＝NetMonitor 木马
5400＝Blade Runner 木马
5401＝Blade Runner 木马
5402＝Blade Runner 木马
5550＝JAPAN xtcp 木马
5554＝假警察蠕虫
5555＝ServeMe 木马
5556＝BO Facil 木马
5557＝BO Facil 木马
5569＝Robo-Hack 木马
5631＝pcAnywhere
5632＝pcAnywhere
5742＝WinCrash 木马
5800＝VNC 端口
5801＝VNC 端口
5890＝VNC 端口
5891＝VNC 端口
5892＝VNC 端口
6267＝广外女生木马
6400＝The Thing 木马
6665＝IRC
6666＝IRC SERVER PORT

6667＝小邮差病毒
6668＝IRC
6669＝IRC
6670＝DeepThroat 木马
6711＝SubSeven 木马
6771＝DeepThroat 木马
6776＝BackDoor-G 木马
6881＝BT 下载
6882＝BT 下载
6883＝BT 下载
6884＝BT 下载
6885＝BT 下载
6886＝BT 下载
6887＝BT 下载
6888＝BT 下载
6889＝BT 下载
6890＝BT 下载
6939＝Indoctrination 木马
6969＝GateCrasher/Priority 木马
6970＝GateCrasher 木马
7000＝Remote Grab 木马
7001＝Windows Messager
7070＝RealAudio 控制口
7215＝Backdoor/SubSeven 木马
7300＝网络精灵木马
7301＝网络精灵木马
7306＝网络精灵木马
7307＝网络精灵木马
7308＝网络精灵木马
7424＝Host Control 木马
7467＝Padobot 木马
7511＝聪明基因木马
7597＝QaZ 木马
7626＝冰河木马
7789＝Back Door Setup/ICKiller 木马
8011＝无赖小子木马
8102＝网络神偷木马
8181＝Zafi 病毒
9408＝山泉木马
9535＝远程管理
9872＝Portal of Doom 木马
9873＝Portal of Doom 木马
9874＝Portal of Doom 木马
9875＝Portal of Doom 木马
9898＝假警察蠕虫
9989＝iNi-Killer 木马
10066＝Ambush 木马
10067＝Portal of Doom 木马
10167＝Portal of Doom 木马
10168＝恶邮差木马
10520＝Acid Shivers 木马
10607＝COMA 木马
11000＝Senna Spy 木马
11223＝Progenic 木马
11927＝Win32. Randin 病毒
12076＝GJammer 木马
12223＝Keylogger 木马
12345＝NetBus 木马
12346＝GabanBus 木马
12361＝Whack-a-mole 木马
12362＝Whack-a-mole 木马
12363＝Whack-a-Mole 木马
12631＝WhackJob 木马
13000＝Senna Spy 木马
13223＝PowWow 聊天
14500＝PC Invader 木马
14501＝PC Invader 木马
14502＝PC Invader 木马
14503＝PC Invader 木马
15000＝NetDemon 木马
15382＝SubZero 木马
16484＝Mosucker 木马
16772＝ICQ Revenge 木马
16969＝Priority 木马
17072＝Conducent 广告
17166＝Mosaic 木马
17300＝Kuang2 木马
17449＝Kid Terror 木马
17499＝CrazzyNet 木马
17500＝CrazzyNet 木马
17569＝Infector 木马
17593＝Audiodoor 木马
17777＝Nephron 木马
19191＝蓝色火焰木马

19864＝ICQ Revenge 木马
20001＝Millennium 木马
20002＝Acidkor 木马
20005＝Mosucker 木马
20023＝VP Killer 木马
20034＝NetBus 2 Pro 木马
20808＝QQ 女友病毒
21544＝GirlFriend 木马
22222＝Proziack 木马
23005＝NetTrash 木马
23006＝NetTrash 木马
23023＝Logged 木马
23032＝Amanda 木马
23432＝Asylum 木马
23444＝网络公牛木马
23456＝Evil FTP 木马
23456＝EvilFTP-UglyFTP 木马
23476＝Donald-Dick 木马
23477＝Donald-Dick 木马
25685＝Moonpie 木马
25686＝Moonpie 木马
25836＝Trojan-Proxy 木马
25982＝Moonpie 木马
26274＝Delta Source 木马
27184＝Alvgus 2000 木马
29104＝NetTrojan 木马
29891＝The Unexplained 木马
30001＝ErrOr32 木马
30003＝Lamers Death 木马
30029＝AOL 木马
30100＝NetSphere 木马
30101＝NetSphere 木马
30102＝NetSphere 木马
30103＝NetSphere 木马
30103＝NetSphere 木马
30133＝NetSphere 木马
30303＝Sockets de Troie 木马
30947＝Intruse 木马
31336＝Butt Funnel 木马
31337＝Back-Orifice 木马
31338＝NetSpy DK 木马
31339＝NetSpy DK 木马
31666＝BOWhack 木马
31785＝Hack Attack 木马
31787＝Hack Attack 木马
31788＝Hack-A-Tack 木马
31789＝Hack Attack 木马
31791＝Hack Attack 木马
31792＝Hack-A-Tack 木马
32100＝Peanut Brittle 木马
32418＝Acid Battery 木马
33333＝Prosiak 木马
33577＝Son of PsychWard 木马
33777＝Son of PsychWard 木马
33911＝Spirit 2000/2001 木马
34324＝Big Gluck 木马
34555＝Trinoo 木马
35555＝Trinoo 木马
36549＝Trojan-Proxy 木马
37237＝Mantis 木马
40412＝The Spy 木马
40421＝Agent 40421 木马
40422＝Master-Paradise 木马
40423＝Master-Paradise 木马
40425＝Master-Paradise 木马
40426＝Master-Paradise 木马
41337＝Storm 木马
41666＝Remote Boot tool 木马
46147＝Backdoor. sdBot
47262＝Delta Source 木马
49301＝Online KeyLogger 木马
50130＝Enterprise 木马
50505＝Sockets de Troie 木马
50766＝Fore 木马
51996＝Cafeini 木马
53001＝Remote Windows Shutdown 木马
54283＝Backdoor/SubSeven 木马
54320＝Back-Orifice 木马
54321＝Back-Orifice 木马
55165＝File Manager 木马
57341＝NetRaider 木马
58339＝Butt Funnel 木马
60000＝DeepThroat 木马
60411＝Connection 木马

61348=Bunker-hill 木马
61466=Telecommando 木马
61603=Bunker-hill 木马
63485=Bunker-hill 木马
65000=Devil 木马
65390=Eclypse 木马
65432=The Traitor 木马
65535=Rc1 木马

A.2 UDP 端口

31=Masters Paradise 木马
41=DeepThroat 木马
53=域名解析
67=动态 IP 服务
68=动态 IP 客户端
135=本地服务
137=NetBIOS 名称
138=NetBIOS DGM 服务
139=文件共享
146=FC-Infector 木马
161=SNMP 服务
162=SNMP 查询
445=SMB(交换服务器消息块)
500=VPN 密钥协商
666=Bla 木马
999=DeepThroat 木马
1027=灰鸽子木马
1042=Bla 木马
1561=MuSka52 木马
1900=UPnP(通用即插即用)
2140=DeepThroat 木马
2989=Rat 木马
3129=Masters Paradise 木马
3150=DeepThroat 木马
3700=Portal of Doom 木马
4000=QQ 聊天
4006=灰鸽子木马
5168=高波蠕虫
6670=DeepThroat 木马
6771=DeepThroat 木马
6970=RealAudio 音频数据
8000=QQ 聊天
8099=VC 远程调试
8225=灰鸽子木马
9872=Portal of Doom 木马
9873=Portal of Doom 木马
9874=Portal of Doom 木马
9875=Portal of Doom 木马
10067=Portal of Doom 木马
10167=Portal of Doom 木马
22226=高波蠕虫
26274=Delta Source 木马
31337=Back-Orifice 木马
31785=Hack Attack 木马
31787=Hack Attack 木马
31788=Hack-A-Tack 木马
31789=Hack Attack 木马
31791=Hack Attack 木马
31792=Hack-A-Tack 木马
34555=Trin00 DDoS 木马
40422=Master-Paradise 木马
40423=Master-Paradise 木马
40425=Master-Paradise 木马
40426=Master-Paradise 木马
47262=Delta Source 木马
54320=Back-orifice 木马
54321=Back-orifice 木马
60000=DeepThroat 木马

附录 B　计算机网络常用专业术语英汉对照

ACE　访问控制条目
ADSL　非对称数字用户线路
APIPA　自动私有 IP 地址
AppleTalk　可路由协议组
ARP　地址解析协议
ATM　异步传输模式
AUI　连接单元接口
BRI　基本数率接口
bridge　网桥
CCP　总线应用层协议
CIDR　无类别域际路由选择
CRC　循环冗余校验
CSEC　通信安全机构
CSMA/CD　载波侦听多路访问/冲突检测方法
DHCP　动态主机配置协议
DSL　数字用户线路
DNS　域名服务器
EFS　加密文件系统
Ethernet 以太网
FDDI　光纤分布式数据接口
FTP　文件传输协议
gateway　网关
HDLC　高级数据链路控制
host　主机
HTTP　超文本传输协议
hub　集线器
IANA　因特网分配数字机构
ICMP　因特网控制报文协议
IEEE　电气和电子工程师协会
IGMP　因特网组管理协议
IP　因特网互联协议
IPSec　因特网协议安全
IPX/SPX　因特网分组交换协议/顺序分组交换协议
IRDA　红外线数据协议
ISDN　综合业务数字网
Internet　因特网
ITsec　信息技术安全评价标准
LAN　局域网
LLC　逻辑链路控制
MAC　媒体访问控制
MAN　城域网
modem　调制解调器
MSAU　多站访问单元
NAT　网络地址转换
NCSA　国家计算机安全协会
NetBEUI　扩展用户接口
NetBIOS　增强型用户接口
NIC　网络适配器
NII　国家信息基础建设
NOS　网络操作系统
OSI　开放式系统互连
PAP　密码认证协议
PKI　公用密钥基础结构
PPP　点到点协议
PPTP　点到点隧道协议
PRI　基速率接口
PSTN　公共交换电话网
PVC　永久虚拟回路
QoS　服务质量
RARP　反向地址解析协议
router　路由器
SAP　服务访问点
SLIP　串行线路网际协议
S/MIME　网际邮件扩充协议
SMTP　简单邮件传输协议
SNA　网络体系结构
SNMP　简单网管协议
STP　屏蔽双绞线
switch　交换机(网桥)
TCP/IP　传输控制协议/因特网互联协议
Telnet　远程控制协议
TLS　传输层安全

UDP　用户数据报协议
URL　统一资源定位符
UTP　非屏蔽双绞线
VLAN　虚拟局域网
VPN　虚拟专用网络
WAN　广域网
Web　网页
WINS　Windows 因特网名称服务
WLAN　无线局域网
WWW　万维网
X.25　分组交换协议

参 考 文 献

[1] 黄智诚，等. 计算机网络技术基础[M]. 北京：地质出版社，2001.
[2] 谢希仁. 计算机网络(第四版) [M]. 北京：电子工业出版社，2003.
[3] 逯昭义. 计算机网络体系结构——计算机网络原理[M]. 北京：清华大学出版社，2003.
[4] 刘四清，等. 计算机网络技术基础教程[M]. 北京：清华大学出版社，2004.
[5] 雷震甲. 计算机网络技术及应用[M]. 北京：清华大学出版社，2005.
[6] 向隅. 计算机网络基础[M]. 北京：清华大学出版社，2009.
[7] 张震，等. 计算机网络技术实用教程[M]. 北京：清华大学出版社，2009.
[8] 张少军. 计算机网络与通信技术[M]. 北京：清华大学出版社，2012.
[9] 李毅驰. Windows 2000 Server 网络系统与服务[M]. 北京：清华大学出版社，2001.
[10] 杨云. Windows Server 2003 组网技术与实训[M]. 北京：人民邮电出版社，2007.
[11] 柳青. 网络操作系统应用实验与实训[M]. 北京：高等教育出版社，2007.
[12] 莫有权，等. Windows Server 2008 服务器架设与网络配置[M]. 北京：清华大学出版社，2011.
[13] 黄中伟. 计算机网络管理与安全技术[M]. 北京：人民邮电出版社，2006 .
[14] 李艇. 计算机网络管理与安全技术[M]. 北京：高等教育出版社，2007.
[15] 李展. 计算机安全超级工具集[M]. 北京：清华大学出版社，2009.
[16] Michael T. Goodrich，Roberto Tama. 计算机安全导论[M]. 北京：清华大学出版社，2012.